

連絡とれるくん ver. 1.19

SAML&OIDC 設定・操作ガイド



2020年07月

株式会社 PhoneAppli

NTT Communications 株式会社

目次

1 はじめに	3
2 認証方式の切り替え	4
2.1 認証方式について	4
2.2 動作確認済み IdP	5
2.2.1 SAML 認証において動作確認済みの IdP	5
3 Service Provider としての仕様	6
3.1 SAML 認証時の SP としての仕様	6
3.2 OIDC 時の SP としての仕様	8
4 管理者による SAML 認証の設定	9
4.1 SAML 認証の設定	9
4.2 メタデータについて	10
5 管理者による OIDC の設定	11
5.1 OIDC の設定	11
6 SAML 認証や OIDC 利用時のユーザの認証について	13
6.1 SAML 認証や OIDC 利用時のユーザ単位でのローカル認証設定	13
7 スマホアプリからのログイン状態保持期間について	14
7.1 スマホアプリからのログイン状態保持期間の変更	14
8 ユーザのログイン操作	15
8.1 PC ブラウザでのログイン手順	15
8.2 スマホアプリでのログイン手順	16

改訂履歴表

改訂年月日	頁	項番/項目	改訂内容
2019.02.25			新規作成
2019.04.03	P.11		SSO 用ログインの URL を修正
2019.04.03	P.11		SSO 用ログイン画面から通常ログイン画面への戻り方を追加
2019.04.22	P.12		SSO 用ログインの URL を修正
2019.04.22	P.4		「3.1 SAML 認証時の SP としての仕様」に “SAML Request 時の User-Agent”情報を追加
2019.04.22	P.3		対応 IdP を追加
2019.04.22	P.11		「7 スマホアプリからのログイン状態保持期間について」を追加
2019.04.22	P.14		画面修正に合わせて内容を修正

2019.07.31	P.3		「② SAML 認証」において検証済み認証サービスに「ID Federation」を追加
2019.08.08	P.7		画面ショットを修正
2019.11.30	全体		SAML Response 内の署名位置対応改修に伴い全体を修正
2020.05.15	全体		Office 365→Microsoft 365 変更
2020.07.31	P.3		注意事項を追加
	P.9-12		ログアウトおよびセッションタイムアウト後 URL についての追記

1 はじめに

この度は、Web 電話帳「連絡とれるくん」をご利用いただきまして、誠にありがとうございます。本書は、「連絡とれるくん」の「SAML 認証」または「OpenID Connect」をご利用いただく際の設定・操作ガイドです。

2 認証方式の切り替え

2.1 認証方式について

「連絡とれるくん」では、認証方式を以下の3種類に切り替えることが可能です。

① ローカル認証 & M365 SSO

「連絡とれるくん」内でパスワードを管理するローカル認証と、Microsoft 365 を利用したシングルサインオンを併用できます。デフォルトではこちらが選択されています。

② SAML 認証

特定の認証サービス（以下、IdP と表記します）に対して SAML による認証を実行します。さらに、SAML 認証を設定後、特定のユーザのみローカル認証を行うこともできます。

※2019年12月現在、動作確認を実施している IdP は「2.2.1 SAML 認証において動作確認済みの IdP」を参照ください。

③ OpenID Connect（以下、OIDC と表記します）

特定の IdP に対して OIDC による認証を実行します。さらに、OIDC を設定後、特定のユーザのみローカル認証を行うこともできます。

※2019年12月現在、ID/PW を用いた標準的な OIDC で動作確認を実施している IdP は「CloudGate UNO」のみとなります。

本書では、上記より「② SAML 認証」と「③ OpenID Connect」における Service Provider（以下、SP と表記します）としての仕様と、「連絡とれるくん」管理者側での設定、並びにユーザによる認証手順について説明します。

※本機能は、連携する IdP の情報が必須となります。どのような情報が必要かは、IdP 担当者にご確認ください。

※IdP の仕様によっては連携できない場合があるため、担当営業にご相談ください。

※認証設定が完了すると、管理者アカウントも SAML 認証、または OIDC による認証を行うようになります。IdP 側に、管理者アカウントと同等のアカウントを用意してください。

※フォンアプリ「Card Assist」（PACA）、MFP 連携機能、また一部の連携機能は SAML 認証、及び OIDC に対応していないため、認証設定が完了すると利用不可となります。

※「連絡とれるくん」iPhone アプリはクライアント(デバイス)証明書を利用した SAML 認証、及び OIDC に対応しておりません。

※IdP としての機能(端末制限など)を組み合わせた場合の動作確認は実施しておりません。

2.2 動作確認済み IdP

以下が動作確認済みの IdP となります。ただし、ID/PW を用いた標準的な認証のみ動作を確認しております。IdP 側の機能と組み合わせた場合の動作は未確認であるため、必ずご利用前に実環境での動作確認を行ってください。

2.2.1 SAML 認証において動作確認済みの IdP

認証サービス (IdP)	連絡とれるくんクライアント				
	Internet Explorer 11	Microsoft Edge	Google Chrome	iOS 13	Android 9
CloudGate UNO	○	○	○	○	○
HENNGE ONE	○	○	○	○	○
Azure AD	○	○	○	○*3	○*3
ADFS	○*1	○*1	○	○	×*2

*1 ADFS は環境(Windows としての機能)の影響を受けるため、必ずご利用前に実環境での動作確認を行ってください。

*2 Android アプリは自己証明書に対応しておりません。(アプリケーションとしてご利用になれません)

※以下の IdP はベンダ様による、ID/PW を用いた標準的な SAML 認証にて動作確認のご報告があります。

- IceWall SSO
- ID Federation

*3 Azure AD の SAML 認証機能でワンタイムパスワードを有効にしている場合、連絡とれるくんのスマートフォンアプリでのワンタイムパスワード入力が正常に動作しないことを確認しています。

3 Service Provider としての仕様

「連絡とれるくん」の SP としての仕様について記載します。認証方式変更前に、必ず本項と IdP 側の仕様を照らし合わせ、連携可能か確認してください。

3.1 SAML 認証時の SP としての仕様

項目	説明
対応認証形式	<ul style="list-style-type: none"> ■ SP Initiated SSO <ul style="list-style-type: none"> SAML Request <ul style="list-style-type: none"> - HTTP Redirect Binding - HTTP POST Binding SAML Response <ul style="list-style-type: none"> - HTTP POST Binding ■ IdP Initiated SSO <ul style="list-style-type: none"> SAML Response <ul style="list-style-type: none"> - HTTP POST Binding
SAML 認証完了後に表示される連絡とれるくんの URL	<p>https://<お客様環境 URL>/front/top</p> <p>※<お客様環境 URL>はご利用の連絡とれるくんの URL に読み替えてください。</p>
メタデータ有無	有り
対応している NameID Format	<p>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</p> <p>※IdP から返却する「Subject NameID 値」は、任意の形式とすることができますが、必ず連絡とれるくんのログイン ID（メールアドレス形式）を返すようにしてください。</p>
SP エンティティ ID	<p>連絡とれるくん管理者が任意で指定可能。</p> <p>※IdP 側でユニークな値を払い出し、入力してください。</p>
アサーションコンシューマサービス URL	<p>https://<お客様環境 URL>/front/saml/acs</p> <p>※<お客様環境 URL>はご利用の連絡とれるくんの URL に読み替えてください。</p>
ログアウト URL	<p>https://<お客様環境 URL>/front/logout</p> <p>※<お客様環境 URL>はご利用の連絡とれるくんの URL に読み替えてください。</p>
SAML Request 時の User-Agent	<ul style="list-style-type: none"> ■ iPhone アプリ <ul style="list-style-type: none"> User-Agent: eiger-iphone-sso ■ Android アプリ <ul style="list-style-type: none"> User-Agent: eiger-android-sso
SAML Response 時、署名に用いる鍵情報	x509 証明書
SAML Response から、鍵情報を用いた署名を読み取る箇所	<p>IdP 側の仕様に準拠し、以下から選択。</p> <ul style="list-style-type: none"> - レスポンス内 - アサーション内 - レスポンス内&アサーション内 <p>※「レスポンス内&アサーション内」はアンド条件となるため、両方に署名がある前提となります。片側にしか署名が無い場合、SP として署名の読み取りは失敗したと判断しログインできません。</p> <p>※IdP によってサポートされる署名位置に差異があります。</p>

SAML Response 時、「Name ID」以外に追加の属性要否	不要
SAML Response に含める必要のあるユーザー属性	無し
クライアント証明書への対応	PC ブラウザ版、Android アプリはクライアント証明書に対応して認証を実施できますが、iPhone アプリは対応していないため、認証できません。

3.2 OIDC 時の SP としての仕様

項目	説明
OIDC のログイン URL	https://<お客様環境 URL>/front/login ※<お客様環境 URL>はご利用の連絡とれるくんの URL に読み替えてください。
OIDC のリダイレクト URL	https://<お客様環境 URL>/front/oidc/processCode ※<お客様環境 URL>はご利用の連絡とれるくんの URL に読み替えてください。
OIDC のログアウト URL	https://<お客様環境 URL>/front/logout ※<お客様環境 URL>はご利用の連絡とれるくんの URL に読み替えてください。
クライアント証明書への対応	PC ブラウザ版、Android アプリはクライアント証明書に対応して認証を実施できますが、iPhone アプリは対応していないため、認証できません。

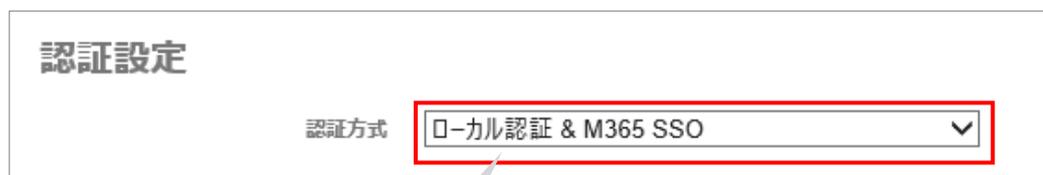
4 管理者による SAML 認証の設定

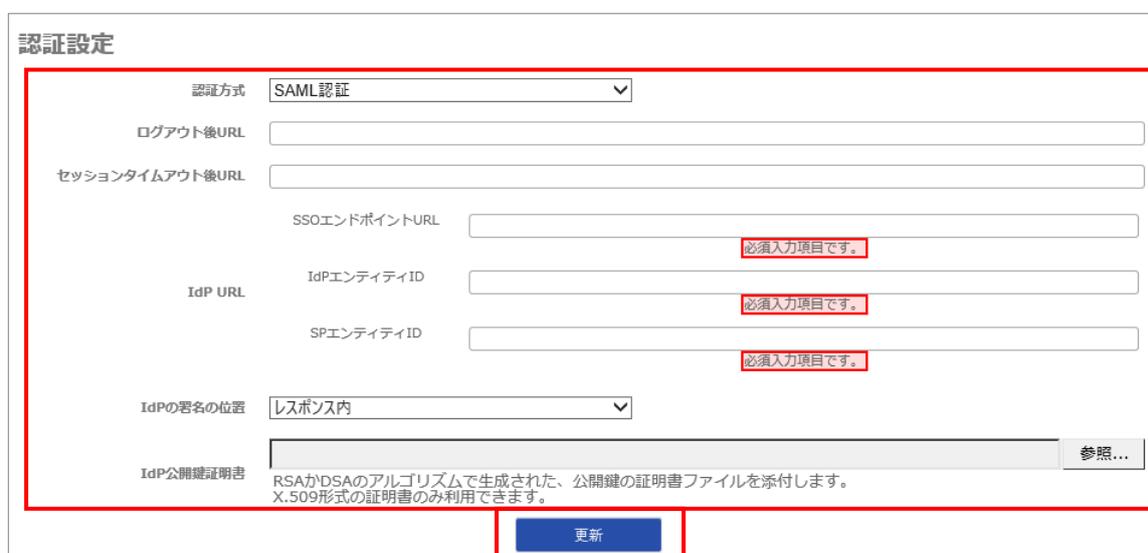
SAML 認証を利用する際の設定手順と注意事項について説明します。

4.1 SAML 認証の設定

以下の設定を行います。

1. 画面右上の [設定] ボタンをクリックします。
2. [管理] をクリックします。
3. [企業情報] タブ→ [社名/ロゴ] タブを選択すると、画面内に「認証設定」のセクションが表示されます。
4. 「認証方式」から [SAML 認証] を選択します。
5. 表示される各種設定項目を入力し [更新] ボタンをクリックします。





■ 設定項目

項目名	説明
SSO エンドポイント URL	SAML リクエストの送信先となる IdP の URL です。
IdP エンティティ ID	IdP 側で発行して入力してください。
SP エンティティ ID	「連絡とれるくん」としては任意の値となります。 必ず IdP 側でユニークな値となる文字列を IdP 側で発行して入力してください。
IdP の署名の位置	IdP 側の仕様に準拠し、以下から選択してください。 <ul style="list-style-type: none"> - レスポンス内 - アサーション内 - レスポンス内&アサーション内 ※「レスポンス内&アサーション内」はアンド条件となるため、両方に署名がある前提となります。片側にしか署名が無い場合、SP として署名の読み取りは失敗したと判断しログインできません。 ※IdP によってサポートされる署名位置に差異があります。
IdP 公開鍵証明書	IdP で発行した証明書 (pem ファイル) をアップロードしてください。 ※RSA か DSA のアルゴリズムで生成された、公開鍵の証明書ファイル ※X.509 形式の証明書のみ利用可能

※ログアウトおよびセッションタイムアウト後 URL については「連絡とれるくん 管理者ガイド」を参照してください。

4.2 メタデータについて

SAML 認証の設定が完了すると、「認証方式」のセクションからメタデータがダウンロードできるようになります。IdP 側で必要な場合、ダウンロードしてご利用ください。

認証設定

認証方式

ログアウト後URL

セッションタイムアウト後URL

SSOエンドポイントURL

IdP URL

IdP エンティティID

SP エンティティID

IdPの署名の位置

IdP公開鍵証明書 参照...

RSAかDSAのアルゴリズムで生成された、公開鍵の証明書ファイルを添付します。
X.509形式の証明書のみ利用できます。

メタデータ ダウンロード

更新

5 管理者による OIDC の設定

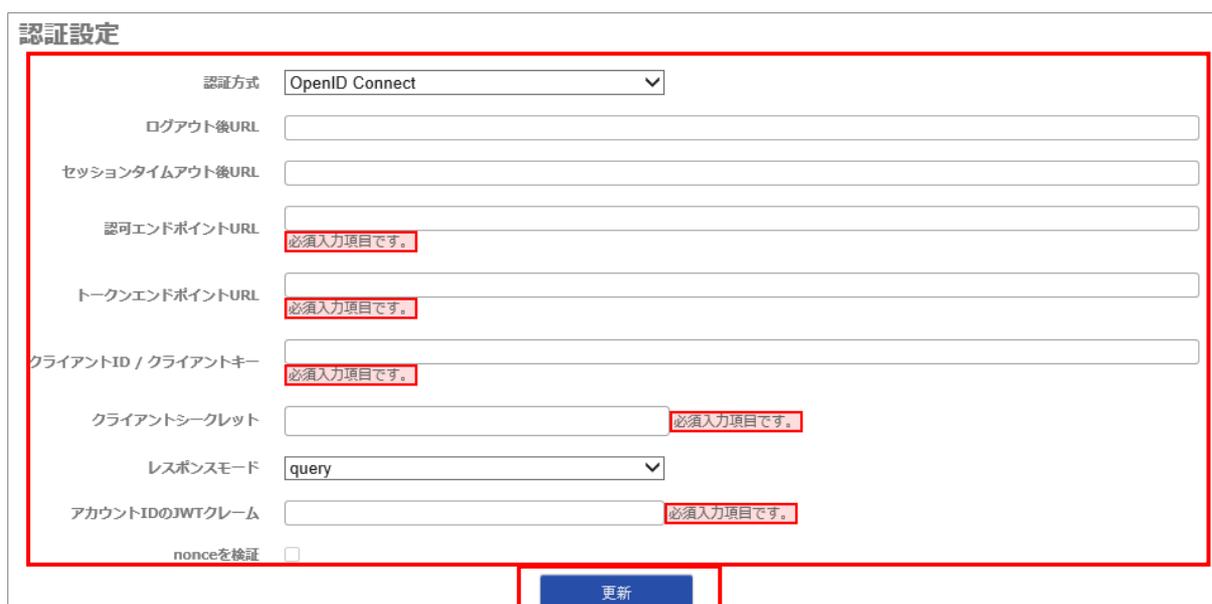
OIDC を利用する際の設定手順と注意事項について説明します。

5.1 OIDC の設定

以下の設定を行います。

1. 画面右上の [設定] ボタンをクリックします。
2. [管理] をクリックします。
3. [企業情報] タブ→ [社名/ロゴ] タブを選択すると、画面内に「認証設定」のセクションが表示されます。
4. 「認証方式」から [OpenID Connect] を選択します。
5. 表示される各種設定項目を入力し [更新] ボタンをクリックします。





■ 設定項目

項目名	説明
認可エンドポイント URL	IdP の認証 URL です。 ※IdP の ID/PW を入力し認証する画面の URL
トークンエンドポイント URL	OIDC トークン URL です。 ※IdP のトークンを発行する URL
クライアント ID / クライアントキー	IdP 側の値です。
クライアントシークレット	IdP 側の値です。
レスポンスモード	「query」と「form_post」から、IdP が対応している方を選択します。 ただし、連絡とれるくんスマホアプリから OIDC を行う場合は、「form_post」を選択していても、強制的に「query」が選択されます。
アカウント ID の JWT クレーム	IdP からの token API のレスポンスにおいて、アカウント ID が含まれる JWT Claim を入力します。 例えば、以下のような JWT Claim の場合、「sub」と入力します。 { "at_hash": "****", "sub": { アカウント ID }, "aud": "****", "azp": "****", "iss": "****", "exp": "****", "iat": "****" }
nonce を検証	チェックを入れることで、OIDC 時、IdP から受け取る ID Token が正しい値か検証できるようになります。 ただし、IdP 側が nonce に未対応の場合はアンチェックとしてください。

※ログアウトおよびセッションタイムアウト後 URL については「連絡とれるくん 管理者ガイド」を参照してください。

6 SAML 認証や OIDC 利用時のユーザの認証について

SAML 認証や OIDC を利用する場合、基本的に全てのユーザは連携設定を投入した IdP に対して認証を行うようになります。

ただし、一部のユーザが連絡とれるくんのローカル認証を利用したい場合、管理者側で設定を行うことができます。

6.1 SAML 認証や OIDC 利用時のユーザ単位でのローカル認証設定

以下の設定を行います。

1. 画面右上の [設定] ボタンをクリックします。
2. [管理] をクリックします。
3. [ユーザ] タブ → [ユーザ管理] タブを選択し、ローカル認証をさせたいユーザの氏名をクリックします。
4. [ローカル認証] の項目にチェックを入れ、[更新] をクリックします。

※ [新規登録] 時も同様のオペレーションでローカル認証ユーザを作成可能です。

※ ユーザインポート時は「LOCAL_AUTH」列を「1」と指定することで、ローカル認証ユーザとすることができます。

※ [ローカル認証] の項目は、認証設定が「ローカル認証 & M365 SSO」を選択されていても表示され、また、エクスポート時に列として出力されます。ただし、その時は当該項目にどんな値が入っていても、ローカル認証を行う動作となります。

注意事項

管理者アカウントは、ローカル認証を利用することができません。認証設定において「SAML 認証」か「OpenID Connect」を設定すると、管理者アカウントでのログイン時は IdP に対して認証を行うようになります。

そのため、必ず、IdP 側に管理者アカウントと同等のアカウントを用意してください。

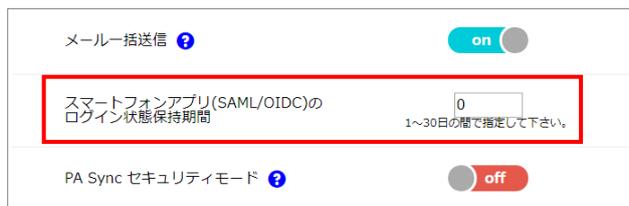
IdP 側に管理者アカウントと同等のアカウントを用意できない場合は、別途、各種管理権限を付与したローカル認証ユーザを作成し、運用してください。

7 スマホアプリからのログイン状態保持期間について

ユーザが SAML 認証や OIDC を利用してスマートフォンアプリからログインした場合、そのログイン状態の保持期間は IdP の設定に依存しません。ログイン状態の保持期間は、連絡とれるくん管理者側で明示的に定義する必要があります。

7.1 スマホアプリからのログイン状態保持期間の変更

[設定] → [管理] → [企業情報] → [スマートフォン] の順に画面遷移をします。



メール一括送信 ⓘ	on
スマートフォンアプリ(SAML/OIDC)のログイン状態保持期間	0 1~30日の間で指定して下さい。
PA Sync セキュリティモード ⓘ	off

「スマートフォンアプリ(SAML/OIDC)のログイン状態保持期間」で指定した期間、スマホアプリのログイン状態が保持されます。

なお、期間を満了すると夜間の定時処理により、スマホアプリからログアウト状態になり、ユーザは次のアクセスから改めて SAML/OIDC によるログインを求められます。

※「スマートフォンアプリ(SAML/OIDC)のログイン状態保持期間」のデフォルト値は 30 日となります。

※本処理は SAML/OIDC 利用時のみの動作となります。

8 ユーザのログイン操作

認証設定において「ローカル認証 & M365 SSO」以外が設定されていて、ログインを試みるユーザの「ローカル認証」にチェックが入っていない場合、ログイン操作は以下の手順となります。

8.1 PCブラウザでのログイン手順

以下の手順でログインをします。

1. PCブラウザにて以下の URL にアクセスします。
https://<お客様環境 URL>/sso
2. ログイン ID を入力します。
3. [次へ] をクリックします。
4. IdP のログイン画面が表示されるため、ID と PW を入力します。
5. 認証成功により、連絡とれるくんのログイン後のトップ画面に遷移します。



ログイン時の注意事項

一度「https://<お客様環境 URL>/sso」にアクセスすると、元々ご利用になっていたログイン画面にはアクセスできなくなるためご注意ください。

※ブラウザのローカルストレージに保存された以下の値を削除し、「https://<お客様環境 URL>/front/login」にアクセスすることで通常のログイン画面に遷移します。

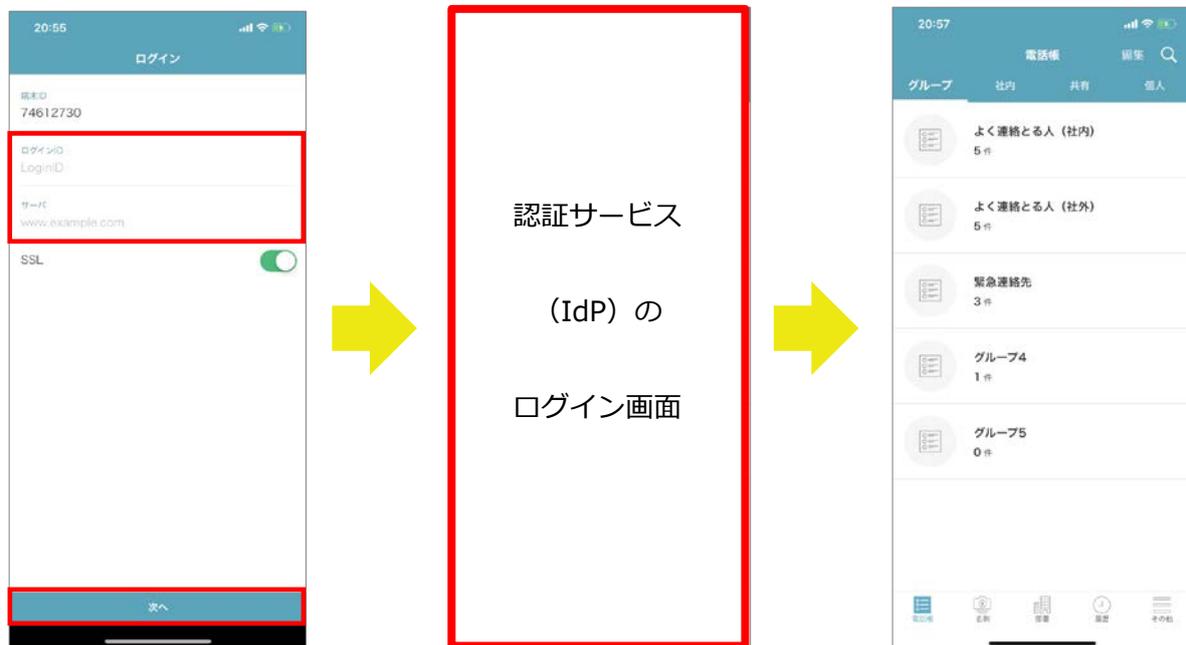
login:mode

8.2 スマホアプリでのログイン手順

以下の手順でログインをします。

1. スマホアプリのログイン画面にて、ログイン ID とサーバ（連絡とれるくんの URL）を入力し、[次へ] をタップします。
2. 認証サービスのログイン画面が表示されるため、ID と PW を入力します。
3. 認証成功により、連絡とれるくんのログイン後の画面に遷移します。

※スマホアプリで初めてアクセスする場合、サービス利用規約への同意を求めるポップアップが表示されます。



ログイン時の注意事項

一度スマートフォンアプリからログインを行うと、「7.1 スマホアプリからのログイン状態保持期間の変更」で定義した期間は、常にログイン状態となります。IdP側でアカウントの停止や、PWの変更をする場合は、連絡とれるくん管理者が以下手順にて、該当ユーザをログアウト状態に変更してください。

1. PCブラウザ版より管理者ログイン後、画面右上の「設定」ボタンをクリックします。
2. 「管理」をクリックします。
3. 「ユーザ」タブ→「ユーザ管理」タブを選択し、該当のユーザの氏名をクリックします。
4. 「スマートフォンアプリ(SAML/OIDC)」の項目の横に表示されている「ログアウトさせる」にチェックを入れ、「更新」をクリックします。

管理 - ユーザ管理

企業情報 部署

ユーザタイプ 基本利用ユーザ

ユーザ画像

ファイルを選択 選択されていません

画像を削除する

端末ID

初回認証を受け付ける

スマートフォンアプリ (SAML/OIDC) ログイン状態 ログアウトさせる

ローカル認証 ローカル認証を利用する ?

本操作により、該当のユーザはモバイルからログアウト状態となります。