# 2要素認証の参考資料

SYNACOR



2024年9月

# 目次

- LDAP属性
- デザイン（動作）概要

# LDAP属性

# LDAP属性（2FA Emailサポート以前から存在）

2要素認証関連

- zimbraTwoFactorAuthEnabled
- zimbraFeatureTwoFactorAuthRequired
- zimbraTwoFactorAuthSecret
- zimbraTwoFactorAuthScratchCodes
- zimbraTwoFactorAuthNumScratchCodes
- zimbraTwoFactorAuthSecretLength
- zimbraTwoFactorAuthHashAlgorithm
- zimbraTwoFactorAuthSecretEncoding
- zimbraTwoFactorScratchCodeLength
- zimbraTwoFactorCodeLength
- zimbraTwoFactorTimeWindowLength
- zimbraTwoFactorTimeWindowOffset
- zimbraTwoFactorAuthScratchCodeEncoding
- zimbraTwoFactorAuthTrustedDeviceTokenLifetime
- zimbraTwoFactorAuthTrustedDevices
- zimbraTwoFactorAuthTrustedDeviceTokenKey
- zimbraTwoFactorAuthTokenLifetime
- zimbraTwoFactorAuthEnablementTokenLifetime
- zimbraFeatureTwoFactorAuthAvailable
- zimbraTwoFactorAuthLastReset
- zimbraTwoFactorAuthLockoutMaxFailures
- zimbraTwoFactorAuthLockoutFailureTime

パスワードリセット機能関連

- zimbraFeatureResetPasswordStatus
- zimbraPrefPasswordRecoveryAddress
- zimbraPrefPasswordRecoveryAddressStatus

# LDAP属性（2FA Emailサポート用に追加）

2要素認証関連

- zimbraTwoFactorAuthMethodAllowed
- zimbraTwoFactorAuthMethodEnabled
- zimbraPrefPrimaryTwoFactorAuthMethod
- zimbraTwoFactorCodeLifetimeForEmail
- zimbraTwoFactorCodeForEmail
- zimbraTwoFactorCodeEmailFrom
- zimbraTwoFactorCodeEmailSubject
- zimbraTwoFactorCodeEmailBodyText
- zimbraTwoFactorCodeEmailBodyHtml
- zimbraTwoFactorAuthEmailCodeLength

詳細は zimbra-attrs.xml参照

# LDAP属性（メールでの2要素認証の設定に用いる主な属性）

事前に設定が必要な主な属性

- zimbraFeatureTwoFactorAuthAvailable：2要素認証の利用可否
- zimbraFeatureTwoFactorAuthRequired：2要素認証の必須有無
- zimbraTwoFactorAuthMethodAllowed：利用可能な2要素認証方法（app and/or email)
- zimbraTwoFactorCodeLifetimeForEmail：メールで送るコードの有効期間
- zimbraTwoFactorCodeEmailFrom：2要素認証コードを含むメールのFromアドレス
- zimbraTwoFactorCodeEmailSubject：2要素認証コードを含むメールの件名
- zimbraTwoFactorCodeEmailBodyText|Html：2要素認証コードを含むメールの本文
- zimbraTwoFactorAuthEmailCodeLength：メールで送るコードの長さ、デフォルト7
  - 認証アプリのコードはzimbraTwoFactorCodeLength 6、復旧用コードはzimbraTwoFactorScratchCodeLength 8

ユーザが2要素認証設定後、自動的にセットされる属性

- zimbraTwoFactorAuthEnabled：2要素認証の利用有無（設定完了の有無）
- zimbraTwoFactorAuthMethodEnabled：2要素認証の方法として設定された方法（app and/or email)
- zimbraPrefPrimaryTwoFactorAuthMethod：第1方法（ログイン時にデフォルトで用いる方法）
- zimbraTwoFactorCodeForEmail：メールで送られたコードと有効期限を暗号化したもの。認証時に利用。

# 設定イメージ　1/2

- zimbraFeatureTwoFactorAuthAvailable：TRUE
- zimbraFeatureTwoFactorAuthRequired：
  - TRUE：2要素認証をユーザが未設定の場合、ユーザ名とパスワードで認証後、2要素認証の設定画面に遷移
  - FALSE：ユーザ名とパスワードでWebクライアントにログイン後、設定画面で2要素認証を設定可能（任意）
- zimbraTwoFactorAuthMethodAllowed
  - app: 認証アプリを利用可能
  - email: メールでのコード送付方法を利用可能
  - app & email：両方利用可能
  - 空：app と見なす

# 設定イメージ　2/2

2要素認証コードを含むメール送信時に適用される設定

- zimbraTwoFactorCodeEmailFrom
  - 空の場合、ユーザのメールアドレスを使用
  - 空でない場合、本属性で指定されたアドレスからメールが送付される。このメールアドレスのアカウントを事前に作成する必要あり。
- zimbraTwoFactorCodeEmailSubject
  - 空の場合、ZsMsgで定義されたデフォルトの文言を使用
  - twoFactorAuthCodeEmailSubject
- zimbraTwoFactorCodeEmailBodyText|Html
  - 空の場合、それぞれZsMsgで定義されたデフォルトの文言を使用
  - twoFactorAuthCodeEmailBodyText
  - twoFactorAuthCodeEmailBodyHtml

備考：メールでの2要素認証の設定時、メールアドレスを確認するためのコードを含むメールは、次の内容となる。

- From：ユーザのメールアドレス
- 件名：ZsMsgで定義された文言
  - twoFactorAuthEmailSubject
- 本文：ZsMsgで定義された文言
  - twoFactorAuthEmailBodyText
  - twoFactorAuthEmailBodyHtml

# デザイン（動作）概要

# ユーザによる2要素認証（認証アプリ）の設定

- Webクライアントログイン後、設定 > アカウント にて、zimbraTwoFactorAuthMethodAllowed で許可された方法を設定可能
  - zimbraTwoFactorAuthMethodAllowed に app が含まれる場合、認証アプリを設定可能
  - zimbraTwoFactorAuthMethodAllowed に email が含まれる場合、送信先メールアドレスを設定可能

- 認証アプリの設定（変更なし）
  1. アカウントのパスワードを入力
  2. コード生成用文字列を認証アプリに入力
  3. 認証アプリに表示されるコードを入力

- メールでの2段階認証も設定した後は、ラジオボタンでどちらの方法をログイン時に第1方法として使用するかを選択可能

# ユーザによる2要素認証（メール）の設定

- Webクライアントログイン後、設定 > アカウント にて、 zimbraTwoFactorAuthMethodAllowed で許可された方法を設定可能
  - zimbraTwoFactorAuthMethodAllowed に email が含まれる場合、メールアドレスを設定可能
- メールの送付先アドレスはzimbraPrefPasswordRecoveryAddressを使用
  - パスワードリセット機能で利用される属性でもある
- メール内容
  - From：ユーザのメールアドレス
  - 件名：ZsMsgで定義された文言
  - 本文：ZsMsgで定義された文言
- パスワードリセット機能 zimbraFeatureResetPasswordStatusとの連動
  - enabledの場合、2要素認証の設定前に、パスワードリセット用アドレスを設定する必要あり。2要素認証の設定時、このメールアドレスが自動補完される。
  - パスワードリセット用アドレスを初期化すると、2要素認証も同時に無効化される
  - disabledの場合、2要素認証の設定時にメールアドレスを手入力
  - メールによる2要素認証を無効化すると、zimbraPrefPasswordRecoveryAddress(Status)は初期化される

# ログイン時の2要素認証

- ユーザ名とパスワードで認証する
- 2要素認証のコード入力画面が表示される
  - デフォルト： zimbraPrefPrimaryTwoFactorAuthMethodで指定された方法
  - 内部動作：「メール」の場合、zimbraTwoFactorCodeForEmailに値がセットされ、コードを含むメールが送信される。「アプリ」の場合、同属性が空になる。
- アプリとメールの両方を設定済みの場合、コード取得方法を変更するリンクが表示される
  - 内部動作：アプリからメールに切り替えると、zimbraTwoFactorCodeForEmailに値がセットされ、コードを含むメールが送信される。メールからアプリに切り替えると、同属性が空になる。
- メールでのコード入力画面では、コードを再送信するリンクが表示される。1回のみクリック可能
  - メールからアプリに切り替え、アプリからメールに再度切り替えると、コードを含むメールが再送信される。再送信リンクが有効になる。
  - 1回目のコード送信、再送にかかわらず、連続送信が localconfig zimbra_two_factor_auth_resend_email_wait_seconds 秒以下のときにはブロックされる
- メールの内容
  - From：zimbraTwoFactorCodeEmailFrom（未設定の場合はユーザのメールアドレス）
  - 件名：zimbraTwoFactorCodeEmailSubject（未設定の場合はZsMsgで定義された文言）
  - 本文：zimbraTwoFactorCodeEmailBodyText|Html（未設定の場合はZsMsgで定義された文言）
- キャンセルボタン押下で最初のログイン画面に戻る

# ログイン時の2要素認証設定（必須時）

- ユーザ名とパスワードで認証する
- 2要素認証の設定画面が表示される
- zimbraTwoFactorAuthMethodAllowedに2つ以上の値がセットされているとき、2要素認証方法を選択する画面が表示される。値が1つの場合は、その設定画面に直接遷移する。
- 認証アプリの場合、パスワード入力後、コード生成用文字列をアプリに入力し、アプリからコードを取得する
- メールの場合、コード送付先メールアドレスとアカウントパスワード入力後、メールアドレス確認コードを含むメールが送付される
  - 再送リンク押下時には、localconfig zimbra_two_factor_auth_resend_email_wait_seconds 秒以下のときにはブロックされる
- 設定完了後、Webクライアントに遷移する