第一回クライアント管理勉強会 【WEB】

プログラム

16:00～18:00　第一部　相談共有・ディスカッション

便利なシステム・ツールを導入する際に、避けて通れないのがユーザ情報の管理。
マスターの形式が異なったり、連携が難しかったり…と悩みをあげたらきりが無い！？

今回は情シスの永遠のテーマである「ユーザ登録・削除」にフォーカス！
課題や解決策を持ち寄り、ディスカッションの中で最適解を探ります。

18:10～19:00　第二部　座談会

第一部、第二部で「聞き足りない」「語り足りない」という方向けに、交流の場をご提供します。

本日の進行メンバー

		
関野 （座長@東京）	嶋口 （座長@大阪）	福田 （PCNW事務局）

Zoom操作・音声ガイダンス

クオリティソフト社　PCNW事務局　川合（かわい）

第一部：相談共有・ディスカッション

はじめに

今回は「ユーザ登録・削除」にフォーカス！

皆さまから事前に沢山のお悩みを共有いただきました

マスター形式が異なる

データ連携が悩ましい

登録ルールが未整備

…等々

今日は皆で課題や解決策を持ち寄り、ディスカッションの中で

最適解を探ります！チャットでのコメントやご意見も大歓迎！

取り組み紹介：中山様

社員の意識改革が省力化のコツ

なかやま

社員の意識改革が省力化のコツ

PCNW

パナソニック映像株式会社

映像制作会社というより 映像コンテンツソリューション会社

Panasonic

総務・デスクチーム

中山 裕盛（なかやま やすもり）

システム導入に対する立場

全社情報システム管理者

ようやく3人情シスまで来ました！

なかやま

社員の意識改革が省力化のコツ

情シスで管理しているアカウント数	300くらい	ユーザ情報やマスター管理の方法			
情シスがユーザ登録を行うシステム数	7	一元管理する何か	○	手入力	○
情シス以外がユーザ登録を行うシステム数	5	データ連携（アプリケーション）	○	その他	×
シングルサインオンの導入状況	導入済(一部)	データ連携（ファイル利用）	×		

取り組み内容

◎2014年より情報システム担当へ着任
- アカウントID取得ルールの統一
- IDとパスワード管理に関する教育
- 工数管理の表面化と可視化
- 情報セキュリティとの連携

◎2020年より複数名でシステム処理開始
- クラウド、PBクラウド利用
- 業務用アカウントIDの運用開始

ポイント・教訓など

◇グループ本社側システムとの関係でSSOが不完全
◇事業場規模が中途半端で自動連携の効果薄
◇パスワードは各社員の自己責任で管理
◇多要素認証の導入
◇ゼロトラスト対策の導入
・・・などなど

でも一番大事なのは、**社員に対する「教育」**です!!

なかやま

社員の意識改革が省力化のコツ

PCNW

社員に対する教育

ひとの話は聞きましょう

わからなかったら訊きましょう

突っ走らずに落ち着いて

取り組み紹介：中原 様

IdPが対応できない部分は自作スクリプトで

中原

IdPが対応できない部分は自作スクリプトで

PCNW

株式会社 ドリコム
ゲーム開発など

DRECOM with entertainment

情報システム部 情報システムグループ
中原　翼（なかはら　つばさ）

システム導入に対する立場
　全社情報システム管理者

ラーメンとプログラムで生きています。

中原

IdPが対応できない部分は自作スクリプトで

情シスで管理しているアカウント数	1000以上	ユーザ情報やマスター管理の方法			
情シスがユーザ登録を行うシステム数	数個	一元管理する何か	○	手入力	○
情シス以外がユーザ登録を行うシステム数	1	データ連携（アプリケーション）	×	その他	×
シングルサインオンの導入状況	導入済(全体)	データ連携（ファイル利用）	×		

取り組み内容

基本的に「人事マスタ => IdP => 各サービス」
の流れでアカウント作成・無効化

一部IdPでアカウント追加できないものを
スクリプトで自動化

→手作業で行う場面が少なくなり、
　ミスの減少 + 作業時間の短縮

ポイント・教訓など

ポイント
・事前に作業手順をまとめることの重要性
・作業内容を一番分かっているのは自分たち

問題点
・スクリプトの管理コスト
・スクリプト書ける人があまりいない

中原

IdPが対応できない部分は自作スクリプトで

スクリプトによる自動化は会社のブログにも記事を書いているので、

よろしければご覧ください。

(「情シス　ぽちぽち作業」とかで検索すれば出てくるはず)

https://tech.drecom.co.jp/ac2020-automation-is/

取り組み紹介：宮腰 様

リコーグループのID管理

宮腰

リコーグループのID管理

PCNW

リコーITソリューションズ株式会社

ビジネスプロセス革新事業部
システムインフラグループ

RICOH
imagine. change.

宮腰　寿之（みやこし　としゆき）

システム導入に対する立場
　全社情報システム管理者

入社以来情報システム一筋

現在はインフラの導入～運用までを担当

宮腰

Office365の導入で新ID管理に切り替え

PCNW

情シスで管理しているアカウント数	250,000	ユーザ情報やマスター管理の方法			
情シスがユーザ登録を行うシステム数	世界で極毎に1	一元管理する何か	○	手入力	×
情シス以外がユーザ登録を行うシステム数	基本的に0	データ連携（アプリケーション）	○	その他	×
シングルサインオンの導入状況	導入済（一部）	データ連携（ファイル利用）	×		

取り組み内容

～2020年4月 従来のID管理
「Notes ID」とOpen LDAPベースの「シングルユーザID」を連携して管理していた。

2020年4月～ 新たなID管理へ
Ofiice365ベースの「統合ID」に切り替え。ID管理は株式会社セシオス製品を採用。
https://seciosslink.com/casestudy/case_01_ricoh

以前からシステム内にIDマスターを持っているものもあるが、連携での対応は変わっていない。
LDAPベースの「シングルユーザID」も一部継続中。

ポイント・教訓など

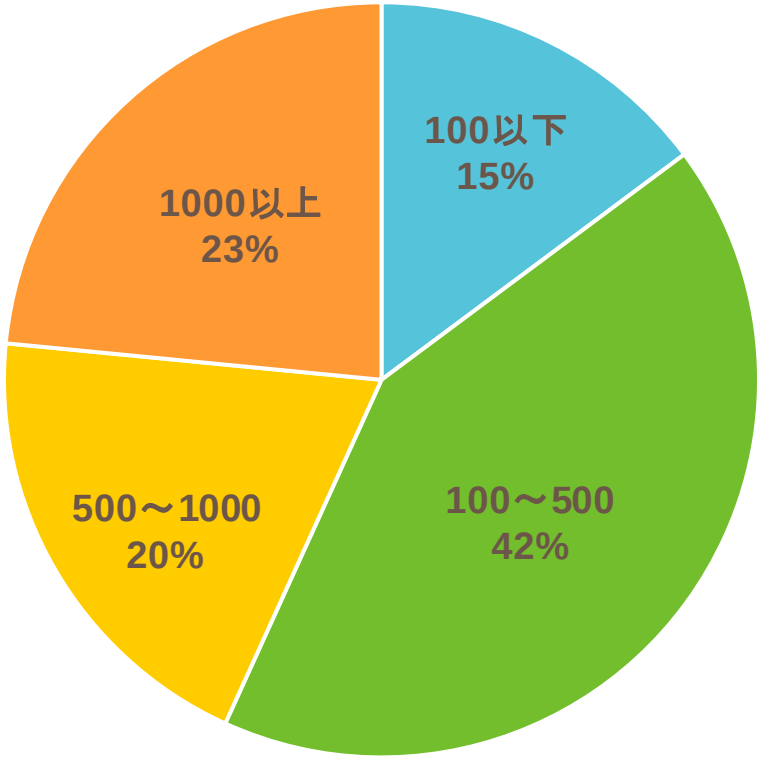
NotesIDとシングルユーザIDの統合管理
NotesIDがベースで社員番号と紐付け。
シングルユーザIDはNotesIDと紐付け。

統合ID
対象は、国内のリコーグループ会社の社員や外部社員のほか、海外のリコーグループ会社の社員や関係者、販売店（ディーラー）にも提供。
・認証基盤はオンプレクラウドに構築。
・アプリケーションからの連携は「SAML」を採用、「OpenID Connect」も利用可能。
・シングルサインオンは限定的に利用中。

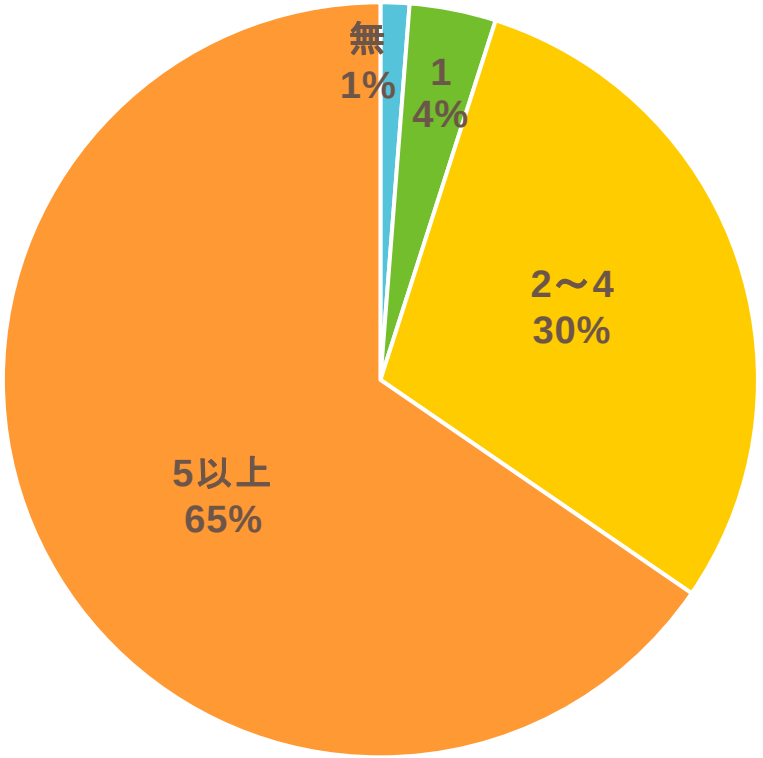
事前アンケート結果

アカウント数やシステム数について

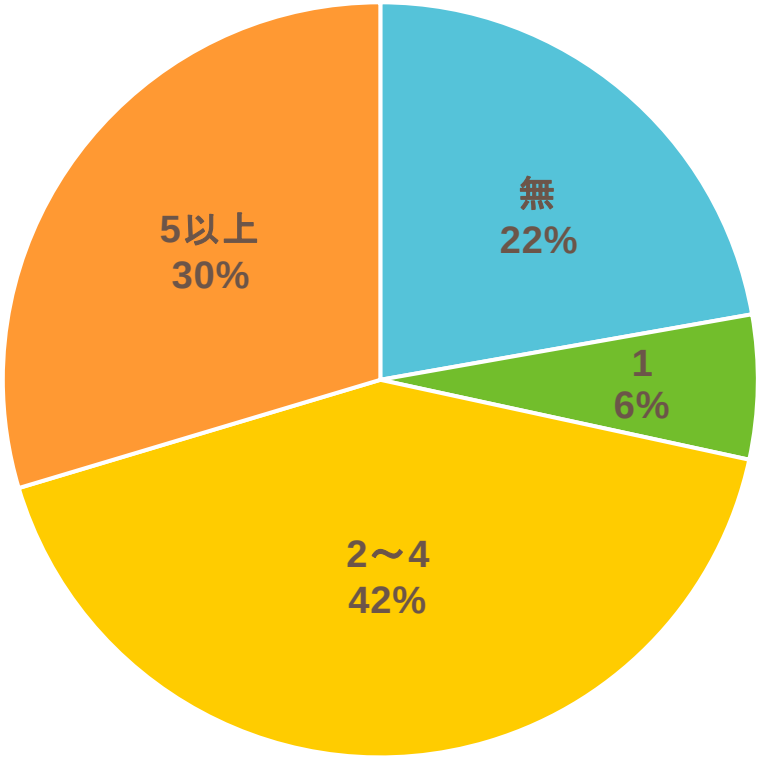
Q1:情シスで管理しているアカウント数



Q2:情シスがユーザ登録を行うシステム数

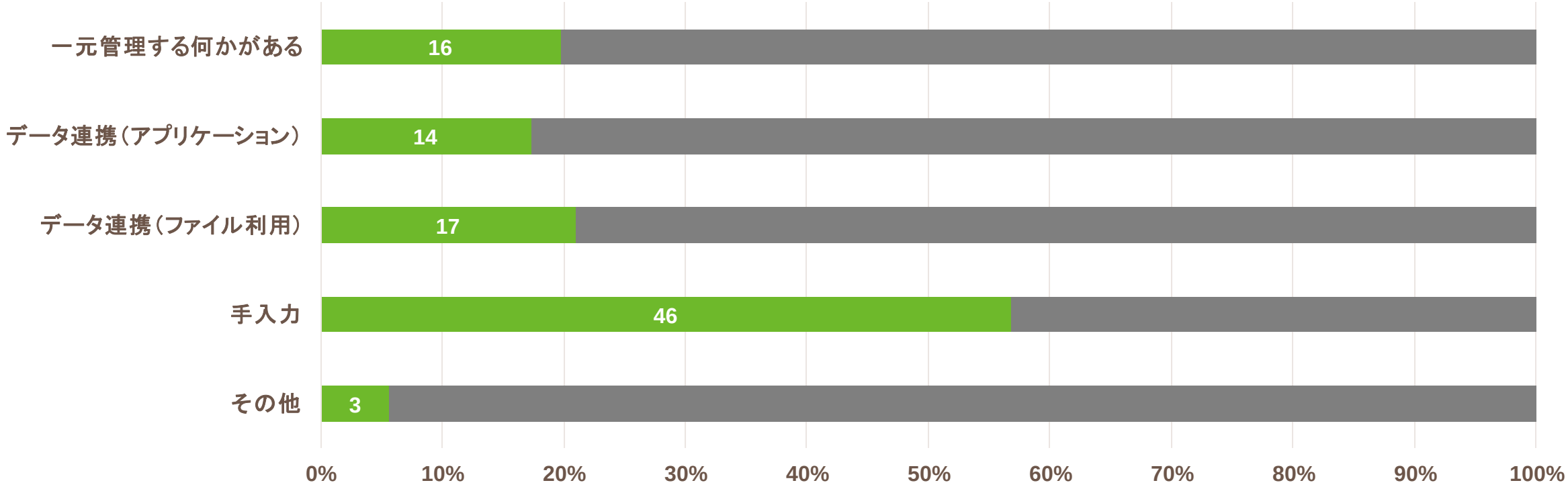


Q3:情シス以外がユーザ登録を行うシステム数



2021/09/09 時点の申込情報で集計：回答者81名

Q4:ユーザ情報やマスター管理の方法を教えてください。

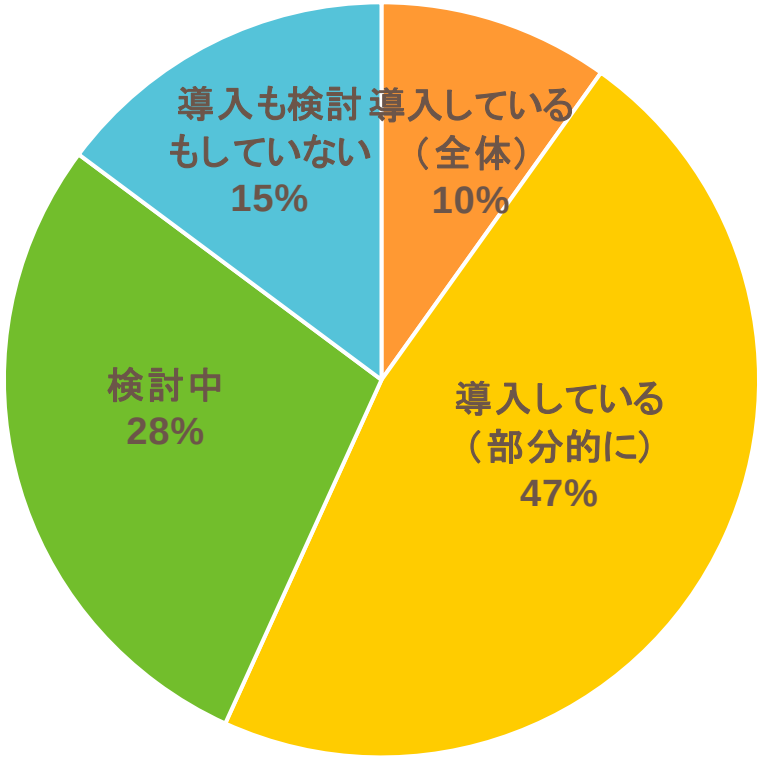


その他	
人事マスターとの連動	kintoneでユーザー情報管理用のアプリを作成しています
人事システムをスタートして運用、マニュアルにて手で入力	手入力のもとはExcel管理

2021/09/09 時点の申込情報で集計：回答者81名

ユーザ情報管理の取り組み

Q5:シングルサインオンの仕組みの導入状況



Q6：ユーザ情報管理について、自社独自の取り組み

手順、チェックリストなどの整備
ルール化はしておりますが、管理は人力です。
人事の退社情報によるユーザー登録の自動無効化を実施
他社がどうかわかりませんが自社の大まかな流れです。 人事が入退社管理システムへ登録 →ADに自動的に登録(所属組織なども保有、社内でスクラッチで作成したシステムは基本ADで認証/権限管理) →googleアカウント登録/別途ユーザー登録が必要なシステムへ自動もしくは半自動で連携
管理部門（人事・総務）と情シス（システム開発部）が分断されているので、週１で打ち合わせを実施している。 アカウント発行依頼はワークフローで申請を起票し、これらのメンバーに横串で回付されるようになっている。
ユーザ情報等が漏えいしたときに備えて、あえてシングルサインオン等を行わない。 時代と逆行していますが…
ありません。 （システムごとに管理が独立しておりＩＤが統合されていない。見かけ上シングルサインオンのような形式になっているが、複数システムのID、PWをテーブルで登録し、ログイン窓に代行入力させているだけ。）

2021/09/09 時点の申込情報で集計：回答者81名

Q8:他の参加者に聞いてみたいことや、共有したい課題①

SSO関連
SSOの利便性とメリット
SSOは導入しているのですが、Googleへのサインインのみに使用して、他サービスはSSO認証をしておりません。
途中からSSO認証に切り替えた際の事例をご紹介いただけると助かります
SSOやSCIMをどこまで適用出来ているか。 ・全●システム(サービス)中、 ■システム(サービス)が導入済み。
・デバイス（社給デバイスのみ適用、スマートデバイスは…等）
連携やSSOのための事前検証方法と本番適用でトラブル発生した場合のリカバリー方法について
古いレガシーのシステムの場合にはSSOが未対応、かつユーザIDの採番ルールも共通化できない。 その場合の工夫ポイントを聞きたい
システム・手法
多くのシステム向けユーザ登録を単一の管理システムに統合して、却って問題が起きたことはありますか？
同じような規模の他社様がどのような管理をしているかが知りたい。その上で今後の課題を考えたい。
当たり前ですが、中途半端に連携させると、「連携しているシステム」と「連携していないシステム」が存在することになり、ユーザーがついていけず、パスワードが共通化されたり簡素化されたりする。やるならがっつりやりたい。 IDaasを使ったプロビジョニングを導入した際に苦労したことがあれば聞きたい。

2021/09/09 時点の申込情報で集計：回答者81名

Q8:他の参加者に聞いてみたいことや、共有したい課題②

ルール・運用
アカウント作成・削除だけでなく、権限付与・削除などの管理
ID情報の作成・削除、管理の効率化について事例があればご教示いただけますでしょうか。
LDAPを使い始めたところで、他にどういうものがあるか、現実的に導入可能かが知りたいです
棚卸実施の有無またその頻度。 氏名入力の際のルール（姓名の間は全角／半角スペースどちら、または別項目にするか等）
グループ会社とマルチドメインによるテナント共有や出向などの対応をどうしているか。 人事との情報共有の方法。
人数が50人以上の会社はどうしているのか知りたい。 退職や権限変更(昇格や部署移動)時、部分的に忘れそうになります。
退職者のアカウント(メールなど)の削除処理のタイミング
・退職済み社員のアカウントの棚卸の方法 ・エクセル台帳以外でのアカウントの効率的な管理
アカウント登録や削除はある程度ルーティンにできたりシステム化できるので何とでもなるのですが、人事異動の際の、人事部門からの情報伝達のトラブル（遅延、連絡なし等）どうされていますでしょうか？ 常にアンテナ張って定期的にこちら側からつつくことで何とかなっていますが、皆さんどうなのでしょうか？

2021/09/09 時点の申込情報で集計：回答者81名