コロナ禍におけるゼロトラストと アイデンティティ管理強化の取り組み例

2021/11/26

auカブコム証券 石川 陽一

ディスクレーマ等

意見は私石川陽一の私見です。

- 機能等の理解が浅い、間違いを含む等の可能性があります。
- 経験上特定のサービス等についてフォーカスする場合があります。シェアしたいのは考え方ですので、適時皆様の環境等の類似ケースに読み替えてください。

会社概要

- 2019/12/2 商号変更
- 口座数 約134万口座
- 従業員数 約180名

石川 陽一 @ishiayaya

Microsoft MVP
Most Valuable Professional

- Microsoft MVP for Data Platform – Power BI Since Sep. 202
- 自称Citizen Developer
- auカブコム
- Power BI, Power Platform, M365, EMS
- 東京・町田在住
- 心臓にIoTデバイスICD埋め込みあり
- セルフ・コミュニティ
  「市民開発者 なってみよう!」 #TryCivicEngr
- コア・参加コミュニティ
  Power BI 勉強会、おうじゃさんといっしょ（Power Apps）

石川陽一（51）の略歴

@ishiayaya

富山出身。奥中(八村塁)、富山高校、同志社大学

1999 日立子会社SEを経て、カブコム立ち上げ
日本初のフルWindows等オープン系金融機関でIT担当

2013 システム監査・内部監査

2013 5ヶ月で-30kg ダイエット

2015 半年で3回致死的不整脈。ICD装着。身障1級

2017/2- サイバー等セキュリティ 同6/29 DDoS攻撃

2019- Microsoft 365 E5 / Power Platform推進

2019/11-2020/3 致死的不整脈多数。ICDと3/13カテーテルアブレーション手術で復活

2020/4 システム統括部門

au カブコム証券
A member of MUFG

個人投資家向け高度プログラミング発注基盤

kabu STATION API

「個人投資家に、デジタルの武器を」

2021/1/27公表 IPA

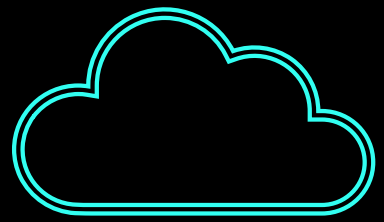
情報セキュリティ 10大脅威 2021

NEW：初めてランクインした脅威

順位	組織	昨年順位
1位	ランサムウェアによる被害	5位
2位	標的型攻撃による機密情報の窃取	1位
3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
4位	サプライチェーンの弱点を悪用した攻撃	4位
5位	ビジネスメール詐欺による金銭被害	3位
6位	内部不正による情報漏えい	2位
7位	予期せぬIT基盤の障害に伴う業務停止	6位
8位	インターネット上のサービスへの不正ログイン	16位
9位	不注意による情報漏えい等の被害	7位
10位	脆弱性対策情報の公開に伴う悪用増加	14位

- 中から外部の接点である「Web」と「メール」が多い
- 境界防御は弱い中をガードする
- 中をモダンで高度にするのは難
- TLPT：中から

止めれれば安全…



“人”等のIDをしっかり、かつ高度化

入社当初からあるもの

エンタープライズIDに関する
手応えは徐々に

- 2017 POWER EGG 
- 2017 アカンサス 
- 2018 OneLogin onelogin
- 2019 M365 E5 

ここ数年の関連する取り組み

- 働き方改革
- 2017/8試行 テレワーク制度(2018/1正式)
  au クラウドPBX 内線機能付iPhone Slack
- 2019/5- M365開始 Teams
- 2019/11- BCP訓練でTeams活用
- 2020/3- コロナ禍でPower Platform活用
  △VPN逼迫、増強、ネット会議時々不安定…

（2019年春）貸与iPhoneの場合

- 「iPhoneで予定も見られないの?…」
- 「上場会社で365を使っていないのは当社ぐらいだ!」

一定のセキュリティがあれば、便利なことを使える

2019年当初はiPhone（iOS）から

AI-OCR が注目されている中、「注文書・請求書のシステム登録自動化」、「申込書のシステム登録自動化」、「社内で保管された大量の文書のデータ化」、「大量アンケートのデータ集計」に活用したいと思いながら、導入方法が分からなかったり、思ったほど ROI が出ないなどで悩んでいる方はいらっしゃいませんか？ AI-OCR を活用し、ROI を達成するためには、OCR の部分だけでなく、その前後の FAX-PDF 化、帳票の振り分け作業、帳票チェック作業など、トータルで有機的に連結された仕組みを構築することが必要です。更に基幹業務システムへの連携は RPA を活用することで自動化することが可能になります。本セミナーではこの「 AI-OCR のトータルサポート」をご紹介するとともに、 AI-OCR による生産性改革を成功させるためのノウハウとクラウド基盤としてなぜAzureが選ばれるのかをお伝えします。
また、この度、TISより新しくリリースした非定型の帳票読み取り AI サービスを紹介し、このサービスを活用した「AI OCR × RPA 」の完成形をご紹介致します。
皆様のご来場を心よりお待ちしております。

【開催日時】 2020年2月12日（水）15:00～17:00

【会場】日本マイクロソフト株式会社 品川本社

【定員】50名

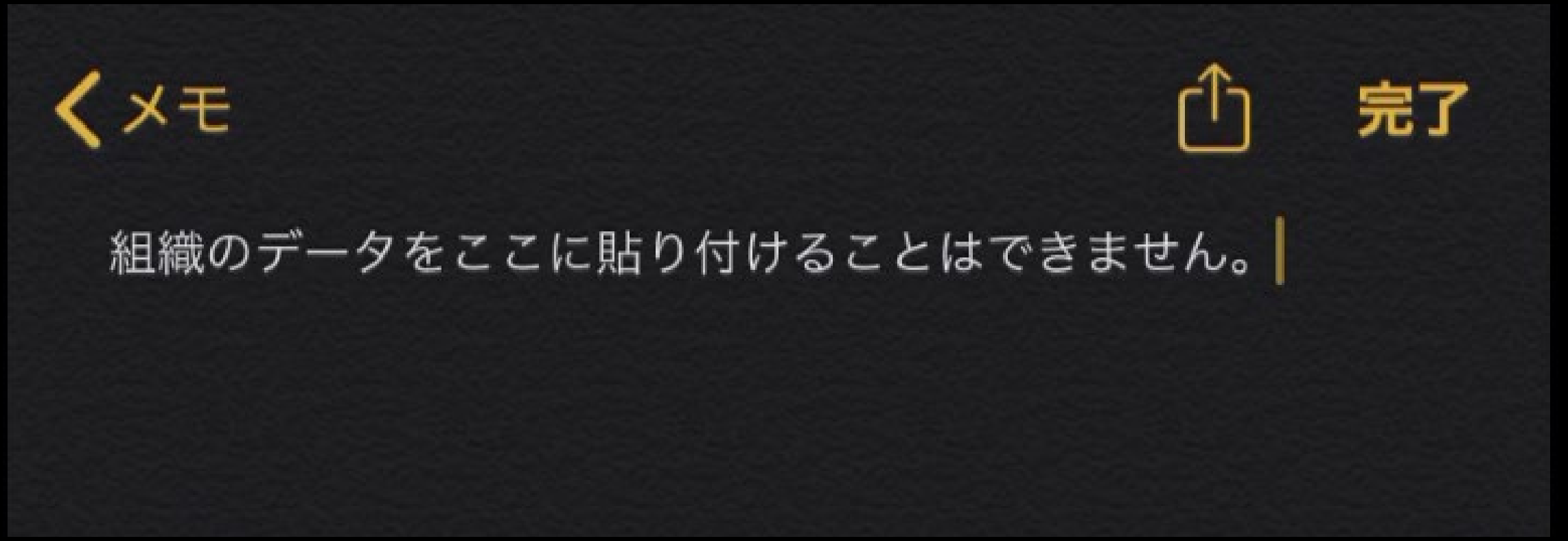
【主催】 TIS 株式会社　【共催】日本マイクロソフト株式会社

本イベントセミナーへのお申込み・詳細情報はこちら

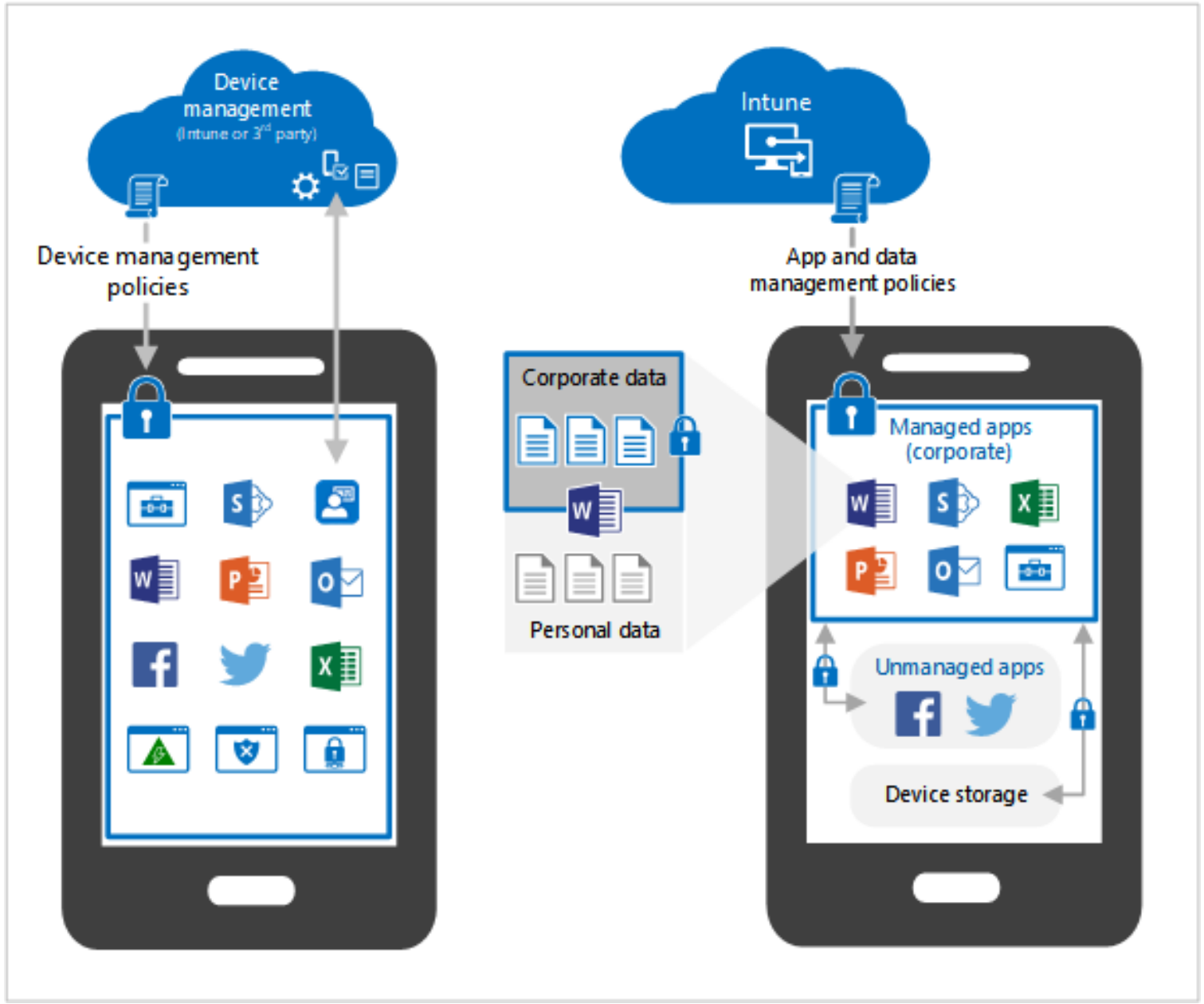
※こちらのリンクはTIS株式会社のページへ進みます

Communication ID：SREMD55684

返信


メモ
完了
組織のデータをここに貼り付けることはできません。

MDM

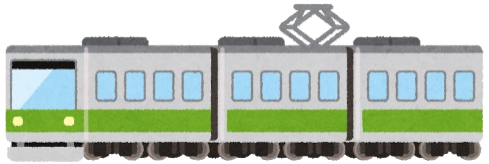


MAM

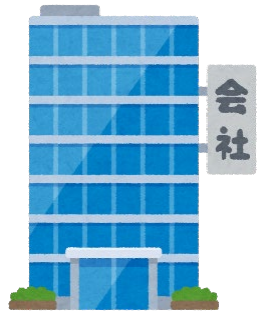
出所「Microsoft Enterprise Mobility + Security (EMS) で BYOD を有効にするための技術の決定事項」より一部抜粋
https://docs.microsoft.com/ja-jp/intune/fundamentals/byod-technology-decisions

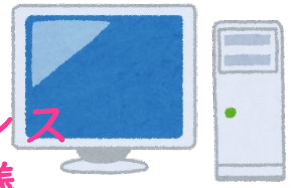
急にきたコロナ禍

ビフォーコロナ



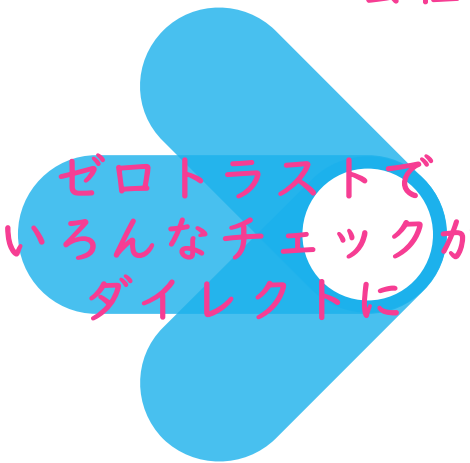
コロナ禍

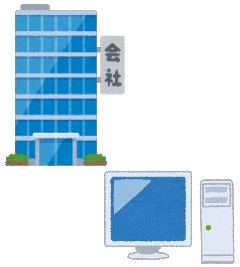




会議室ガラガラ
ソーシャルディスタンス
会社でもネット会議

Withコロナ





E5系の新環境

PCのデバイス管理をiPhone同様にしたい

情報収集・理解・共有

- 日本マイクロソフトさん他
- 現場の部門同士（例 セキュリティとIT）
- 外部の勉強会参加
- 経営陣と共有機会
- 見える化への取り組み

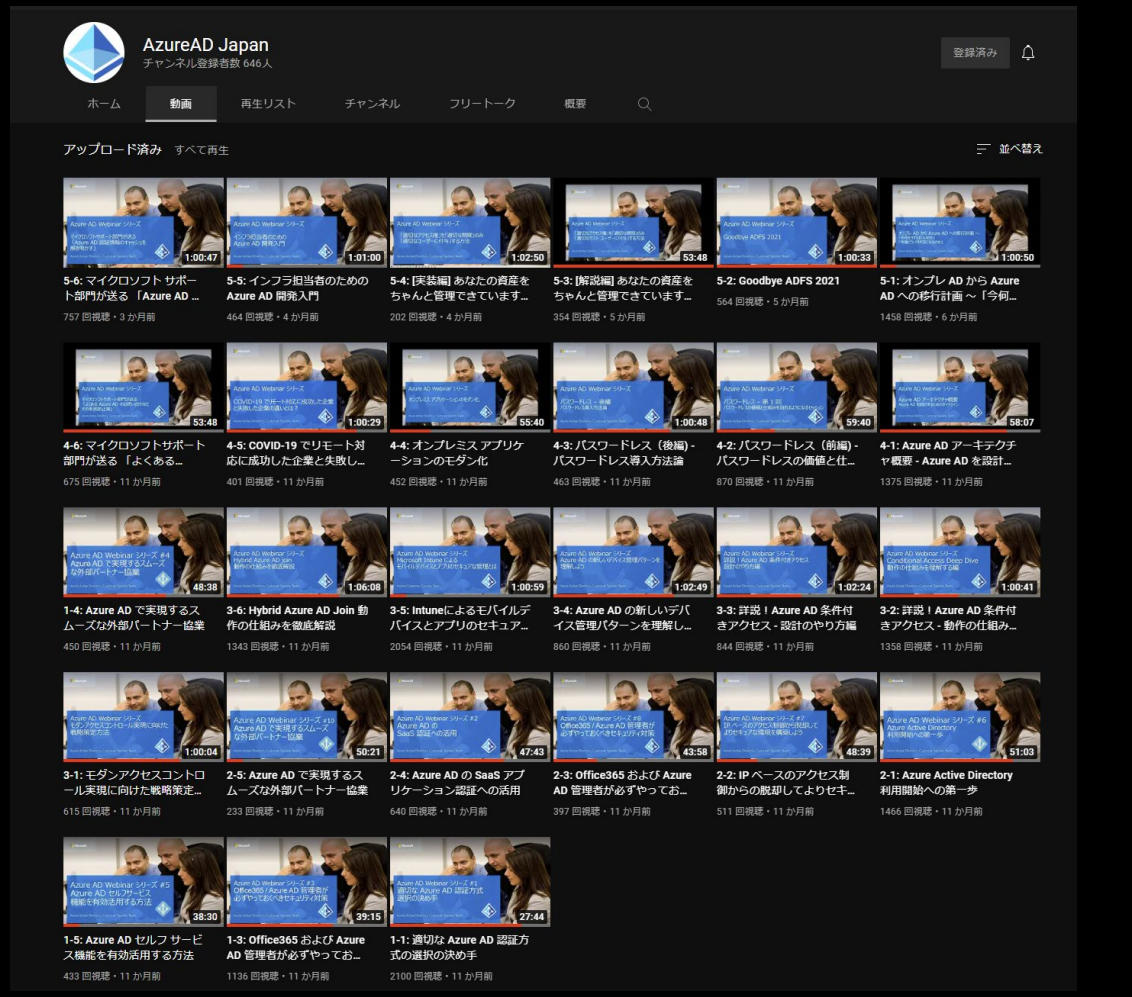
Azure AD Webinar
https://aka.ms/AzureAdWebiner

YouTube
https://aka.ms/AADRecording

スケジュール

Season 5 (2021年 2月 - 5月実施)

#	日時	テーマ	登録リンク	資料
1	2/25(木) 13:30- 14:30	**オンプレ AD から Azure AD への移行計画 ～「今何をすればいいのか」「今後どういう状況になるのか」について** Azure AD とオンプレ AD の運用について良くある疑問について解説いたします	Recording	download QA sheet
2	3/11(木) 13:30- 14:30	**Goodbye ADFS 2021** De:code 2019 で好評をいただいた Goodbye ADFS (http://aka.ms/goodbyeadfsppt) のアップデートセッションです。2020年、たくさんのお客様が Azure AD Staged rollout を用いたフェデレーション環境からの離脱を成功させました。このセッションではフェデレーション環境を離脱することの意義の復習と、最新の機能を用いた移行のデモを交えた実演で皆さんの理解を深めます。	Recording	download QA sheet
3	3/25(木) 13:30- 14:30	**[解説編] あなたの資産をちゃんと管理できていますか？「適切なアクセス権」を「適切な期間」のみ「適切なユーザーに付与」する方法** Digital Trust Summit 2020 で紹介したセッション (https://aka.ms/DigitalTrustSummit2020ELM) の継続セッションです。セキュリティの基本として「必要最小限のアクセス権の付与」「使うときだけアクセス権を付与する」「必要のなくなったアクセス権はすぐに外す」などと言われていますがこれがきっちりとできている企業はどれぐらいいるのでしょうか？このセッションでは Identity Governance の機能が上記課題をどのように解決していくのかを紹介します。	Recording	download QA sheet
4	4/8(木) 13:30- 14:30	**[実装編] あなたの資産をちゃんと管理できていますか？「適切なアクセス権」を「適切な期間」のみ「適切なユーザーに付与」する方法** 前回のセッションで話した Identity Governance の実装方法を紹介します。まずは PoC としてこの動画で紹介する内容をお試しいただき、あなたの環境での有用性をご確認ください。	Recording	download QA sheet
5	4/22(木) 13:30- 14:30	**インフラ担当者のための Azure AD 開発入門** "いま開発しているアプリケーションを Azure AD と連携したい、一体どうしたらよいんですか？"と社内の開発者に聞かれてギクリときたことのある インフラ/ID基盤担当の方はこちらのセッションにご参加ください。 Identity 担当者が押さえておくべきアプリケーション登録のセキュリティ設定やアプリケーションと Azure AD の連携動作フローを解説します。	Recording	download QA sheet
6	5/13(木) 13:30- 14:30	**マイクロソフトサポート部門が送る「Azure AD 認証情報のキャッシュを解き明かす」** Azure AD では認証情報が適切にキャッシュされることによりシングルサインオンを実現しています。利便性は高くなる機能である反面、すべてバックグラウンドで行われる処理であるため、管理者はキャッシュがどのように扱われているのかを疑問に思う事があると思います。このセッションでは Azure AD のトークン情報の扱い方と、様々なシナリオにおいてキャッシュがどのように扱われているのかを明確にしていきます。	Recording	download QA sheet



自社が持つ365ライセンスに何が含まれるのか?

M365

Business Basic

E3

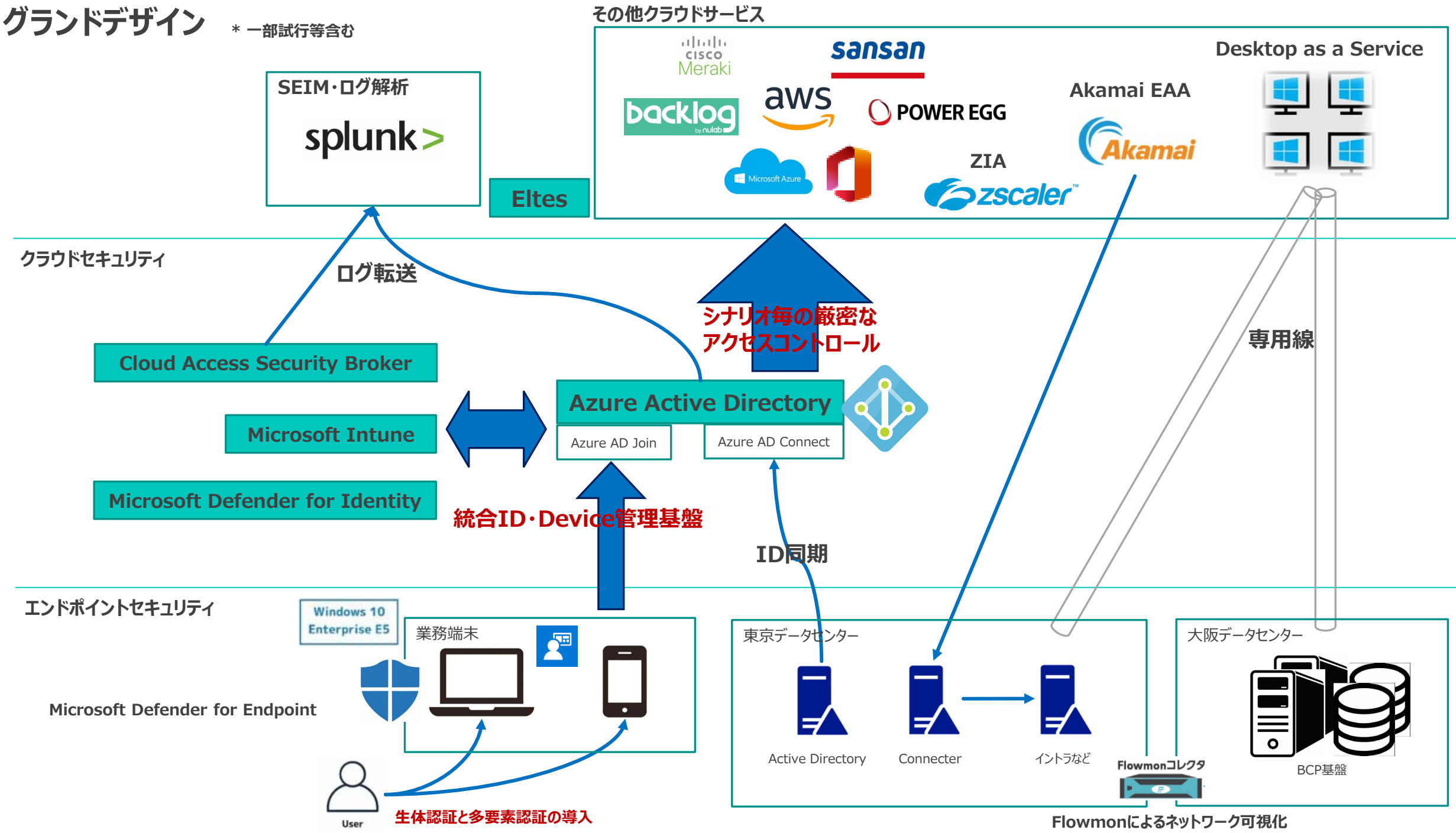
E5

大きく3つのE5

- O365 E5
- EMS E5
- Win10 Ent. E5

グランドデザイン

＊ 一部試行等含む



ゼロ トラスト

特に見直し、強化した3点

1. ID周りをよりよく

2. EDRは優先高

3. 情報の理解・共有等が大事

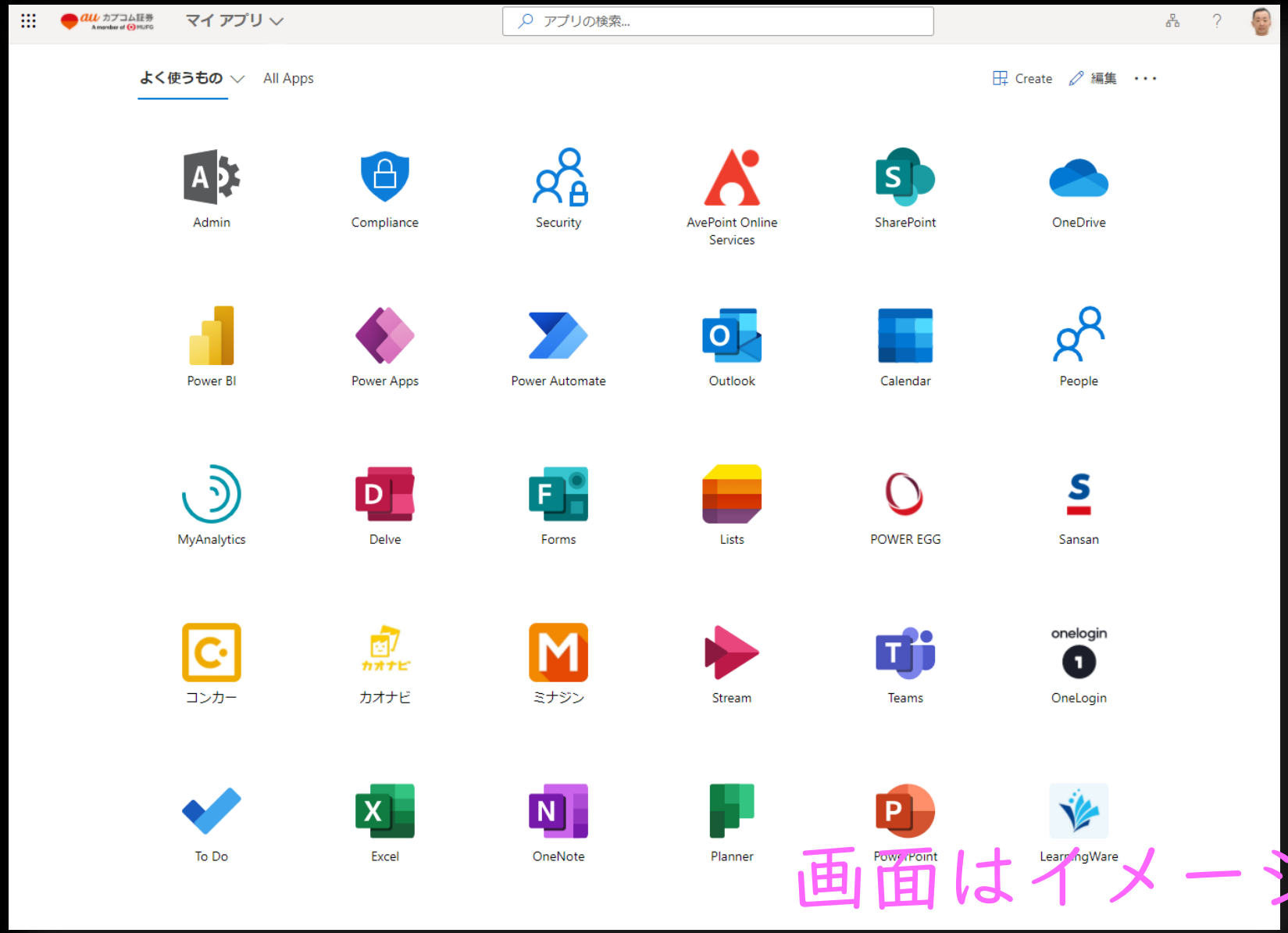
ID周り

- IDaaS

- パスワード→多要素→
  パスワードレス

画面はイメージです

Webサービス毎に、ID・パス…をやめたい



画面はイメージです

IDaaS

人

デバイス

パスワードだけ、は×。代替の見直し

条件付きアクセス

画面はイメージです

EDR

EDR (Endpoint Detection and Response)

EDRへの対応
Endpoint から M365 Defenderへ

Microsoft 365 Defender

ホーム

Microsoft 365 Defender へようこそ

はじめに　次のステップ　フィードバックの送信

脅威に対応し、ID、データ、デバイス、アプリ、インフラストラクチャにわたるセキュリティを管理します。統合エクスペリエンスに関する詳細情報

次へ　閉じる

ガイド ツアー　最新情報　コミュニティ　カードを追加

- ホーム
- インシデントとアラート
- 追及
- アクション センター
- 脅威の分析
- セキュア スコア
- ラーニング ハブ
- 試用版

エンドポイント

- 検索
- デバイスのインベントリ
- 脆弱性の管理
- パートナーと API
- 評価版/チュートリアル
- 構成管理

メールとコラボレーション

- 調査
- エクスプローラー
- 申請
- 確認
- 攻撃活動
- 脅威トラッカー
- Exchange メッセージの追跡
- 攻撃シミュレーションのトレーニング
- ポリシーとルール

- レポート
- 監査
- 正常性
- アクセス許可と役割
- 設定

- その他のリソース
- ナビゲーションのカスタマイズ

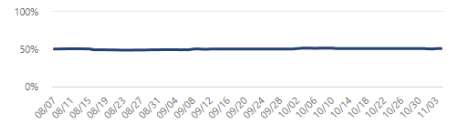
Microsoft セキュア スコア

セキュア スコア: 50.87%

472.58/929 獲得したポイント

Microsoft セキュア スコアは、組織のセキュリティの状態と、その改善の見込みを表します。

前回のスコアの計算: 11/04



ID	81.17%
デバイス	46.04%
アプリ	70%

スコアを向上させる　履歴の表示

危険性のあるユーザー

0 人のユーザーに危険性があります

危険度 - 高　危険度 - 中　危険度 - 低

すべてのユーザーを表示

デバイスのコンプライアンス

29% が非準拠

Intune のデバイス コンプライアンスの状態

準拠　非準拠　猶予期間内　未評価

詳細を表示

検出されたデバイス

5 ネットワーク内で検出されたデバイス

過去 30 日間にアクティブ

ワークステーション

すべてのデバイスを表示

セキュリティ ニュース フィード

Microsoft 365 Defender

A Twitter list by @MsftSecIntel

Product news, security intelligence, and threat research

Microsoft Security Intelligence Retweeted

Tanmay Ganacharya
@tanmayg

Antivirus behavior monitoring is now generally available on Linux
techcommunity.microsoft.com/t5/microsoft-d…

17h

Microsoft Security Intelligence

Embed　View on Twitter

危険性のあるデバイス

0 台のデバイスが危険にさらされて…

デバイス	リスク レベル

詳細を表示

検出されたオンボード対象のデ…

ネットワーク内で検出されたデバイスは完全にオンボードされました。

脅威の分析

0 件のアクティブな脅威

DEV-0237 deploys Ryuk, Conti, and Hive ransomware	0/0
Threat Insights: Win32k elevation of privilege vulnerability (CVE-2021-40449) exploited	0/0
ZLoader delivered via ad fraud	0/0

アクティブなアラート　解決済みのアラート　アラートはありません

その他を表示

脅威が検出されたユーザー

脅威が検出されたユーザー

ユーザー	アラート
Yoichi Ishikawa	2

デバイスの正常性

個の特権 OAuth アプリ

アクティブなマルウェアが存在…

画面はイメージです

Unsanctioned cloud app access was blocked

ishidesktop2021 Risk level Informational
Data sensitivity:機密

azuread\ishiayaya

ALERT STORY

Expand all

[6932] **explorer.exe**

[26884] **msedge.exe** --profile-directory=Default

[27772] **msedge.exe** --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1928,7545749152291906316,10613680118878403 3...

Network connect

Outbound connection from 192.168.1.19:53873 to 23.60.108.211:443

Unsanctioned cloud app access was blocked Informational New Detected

Details

Unsanctioned cloud app access was blocked

Informational **New**

See in timeline | Link to another incident | Assign to me

Manage alert

Classify this alert — True alert | False alert

Status: New

Classification: Select classification...

Alert details

Incident	Unsanctioned cloud app access was blocked on one endpoint (open in Microsoft 365 Defender)
Detection source	Custom TI
Category	SuspiciousActivity
First activity	2021/08/20 13:44:28
Last activity	2021/08/20 13:44:28
Generated on	2021/08/20 13:45:53
Assigned to	(Unassigned)

Alert description

Microsoft Cloud App Security blocked an attempt to access an unsanctioned app.

Alert recommended actions

A. Validate the alert and scope the suspected breach.

画面はイメージです

見える化

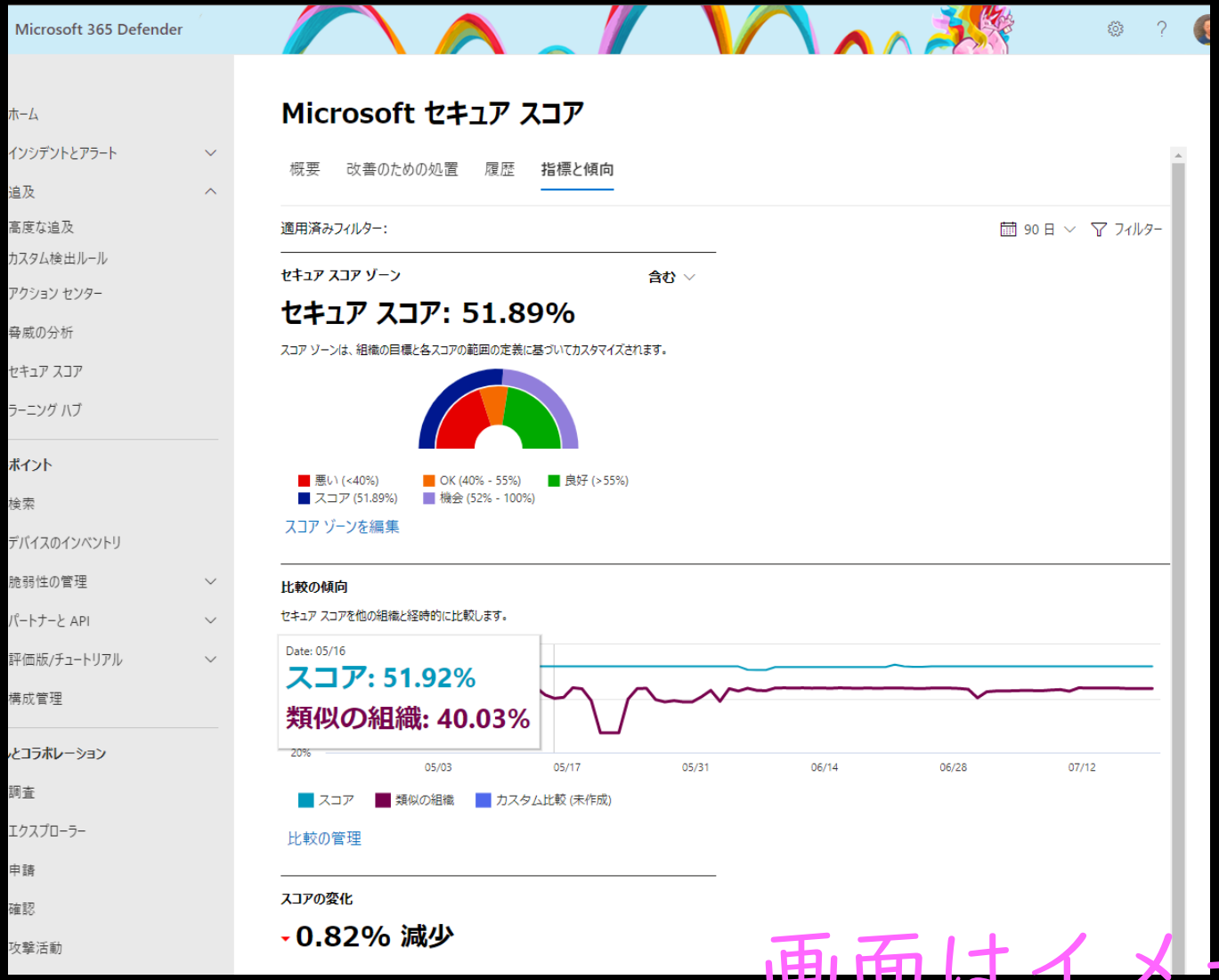
画面はイメージです


Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
ホーム > Azure Sentinel
Azure Sentinel | ハンティング
選択したワークスペース: 'sentinel-ishiayaya'
検索 (Ctrl+/)
最新の情報に更新
過去 24 時間
新しいクエリ
すべてのクエリを実行する (プレビュー)
列
ガイドとフィードバック
全般
概要
ログ
ニュースとガイド
脅威管理
インシデント
ブック
ハンティング
ノートブック
エンティティの動作
脅威インテリジェンス (プレビュー)
構成
データ コネクタ
分析
ウォッチリスト
オートメーション
ソリューション (プレビュー)
コミュニティ
設定
141 / 195
アクティブ/合計クエリ
0 / 0
結果数/クエリの実行回数
0
ライブストリームの結果
0
ブックマーク
クエリ
ライブストリーム
ブックマーク
0 Reco...
0 Reso...
31 Initia...
1 Exec...
1 Persi...
0 Privil...
1 Defe...
2 Cred...
2 Disc...
1 Later...
1 Colle...
1 Com...
クエリの検索
方針 : Initial Access
フィルターの追加
クエリ
プロバイダー
データ ソース
結果
結果の差分 (プレビ...
Failed Login Attempt by Expi... Microsoft SecurityEvent +1
Multiple Password Reset by ... Microsoft AuditLogs +3
Rare domains seen in Cloud ... Microsoft AuditLogs +2
Exploit and Pentest Framew... Microsoft W3CIISLog +2
Anomalous sign-in location ... Microsoft SigninLogs
Attempts to sign in to disabl... Microsoft SigninLogs
Attempts to sign in to disabl... Microsoft SigninLogs
Inactive or new account sign... Microsoft AuditLogs +1
Login attempts using Legacy... Microsoft SigninLogs
Failed attempt to access Azu... Microsoft SigninLogs
Anomalous Azure Active Dir... Microsoft SigninLogs
Azure Active Directory signi... Microsoft SigninLogs
画面はイメージです

見える化

画面はイメージです

当社のスコアは？



画面はイメージです

ローコードアプリやBIの利用

ローコード

テレワーク・時差出勤管理
Ver1.03

石川 陽一さんの登録状況

2020/04/03
テレワーク
07:30-16:30

2020/04/02
テレワーク
07:30-16:30

2020/04/01
テレワーク
06:00-15:00

2020/03/31
出社
07:30-16:30

2020/03/26
テレワーク
06:00-15:00

データ登録

日付
2020/04/06

場所等
テレワーク

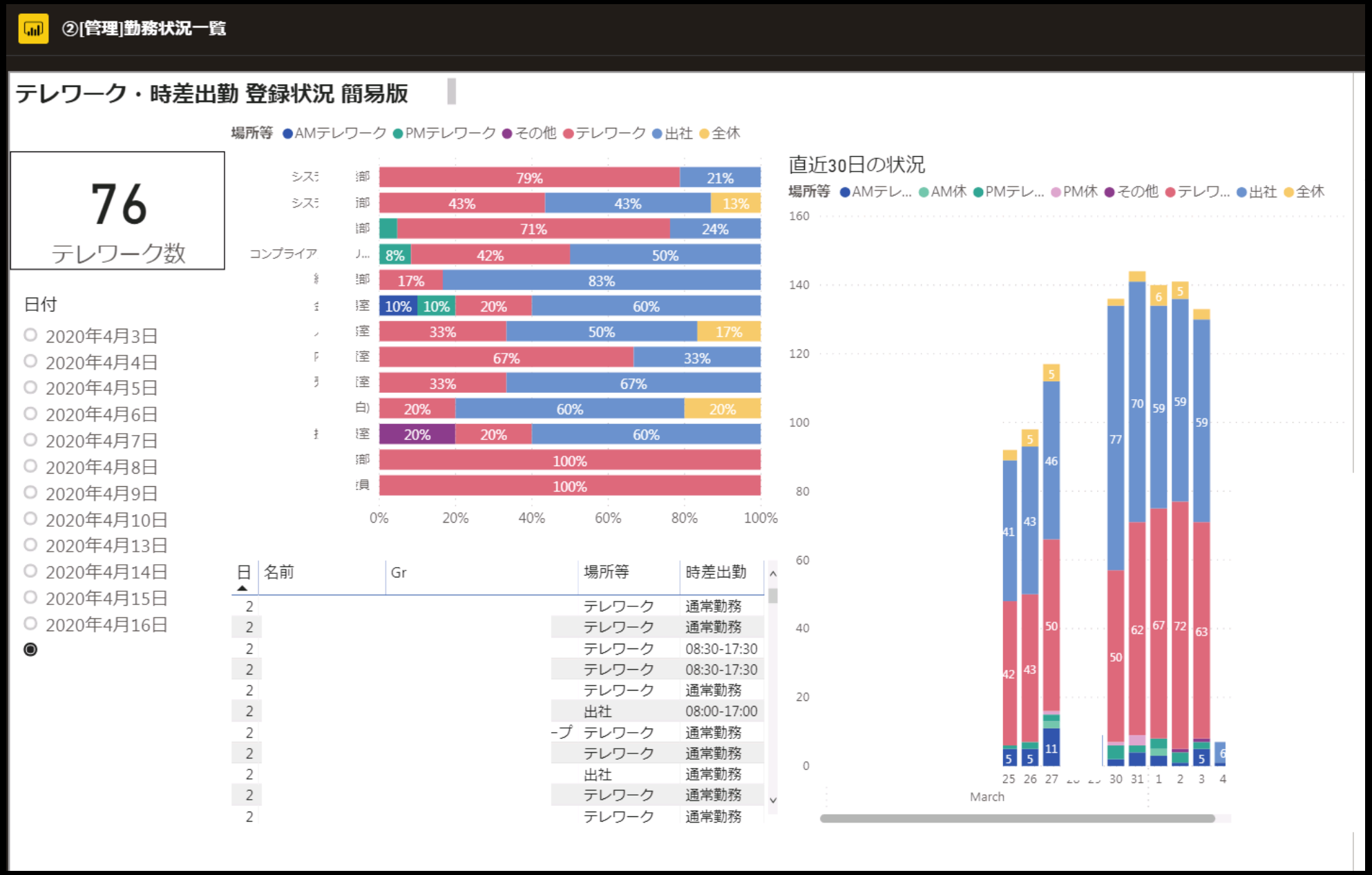
時差出勤
07:30-16:30

ローコード


開発案件管理（案件起案：企画概要~プロジェクト承認書）
案件起案
着手工程・成果物（工事中）
開発進捗
予算管理（工事中）
検索条件を入力してください
すべて
未起票
未承認
承認済み
否認
72件
20-029：シス開発部・IT戦略G
Prj承認書
テスト20200805-005
20-028：シス開発部・IT戦略G
エントリー票
テスト20200805-004
20-027：シス開発部・IT戦略G
エントリー票
テスト20200805-003
企画概要申請画面へ
編集・承認依頼画面へ
申請承認状況
ステータス
起案期限
起案日
企画概要
相談済み

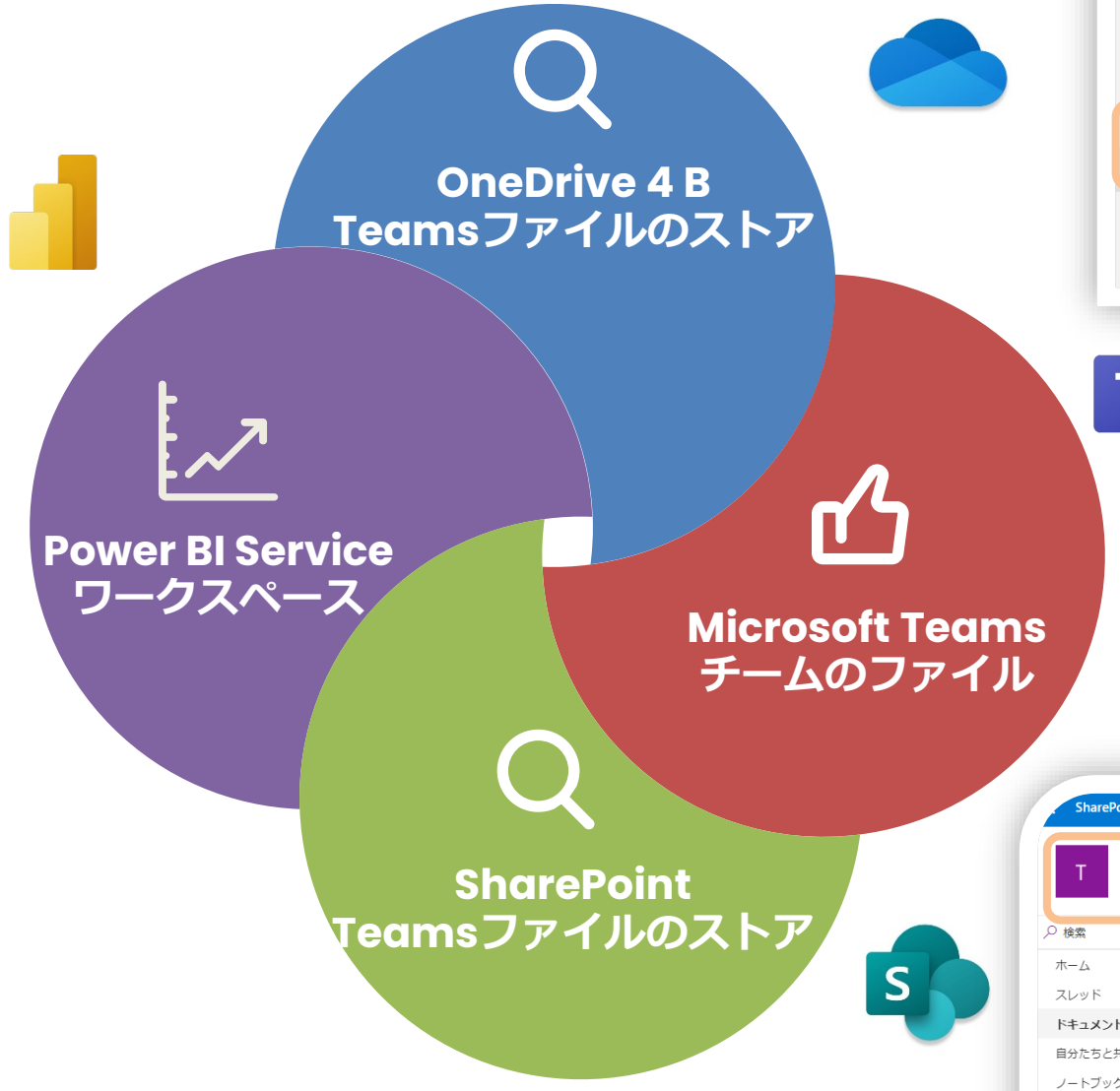
2020/08/06
エントリー票
承認済み
2020/08/05
2020/08/06
プロジェクト承認書
承認未済
2020/08/05
案件情報
案件番号
案件種別
管理 LV
20-029
制度改正
案件名

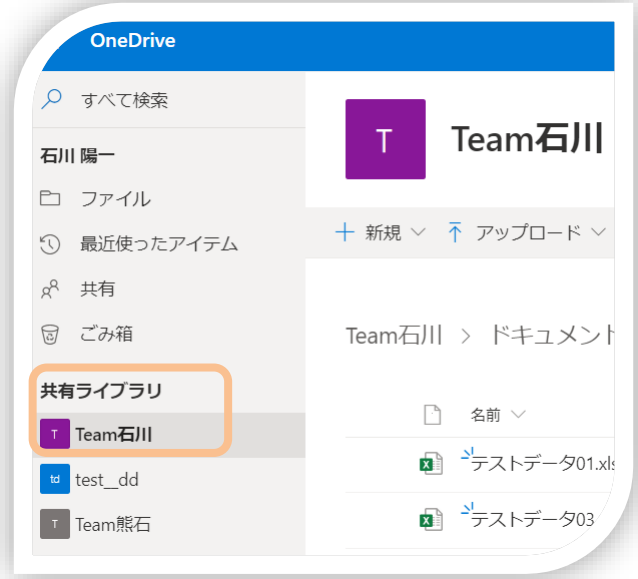
見える化

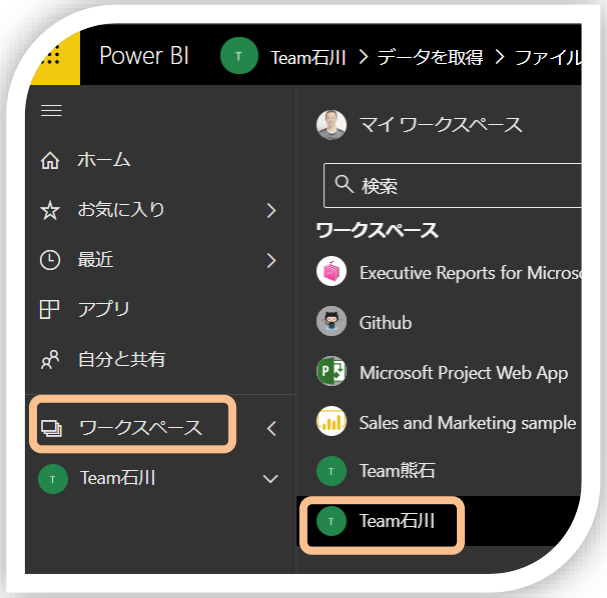

②[管理]勤務状況一覧
テレワーク・時差出勤 登録状況 簡易版
場所等 AMテレワーク PMテレワーク その他 テレワーク 出社 全休
76
テレワーク数
日付
2020年4月3日
2020年4月4日
2020年4月5日
2020年4月6日
2020年4月7日
2020年4月8日
2020年4月9日
2020年4月10日
2020年4月13日
2020年4月14日
2020年4月15日
2020年4月16日
79% 21%
43% 43% 13%
71% 24%
8% 42% 50%
17% 83%
10% 10% 20% 60%
33% 50% 17%
67% 33%
33% 67%
20% 60% 20%
20% 20% 60%
100%
100%
0% 20% 40% 60% 80% 100%
日 名前 Gr 場所等 時差出勤
2 テレワーク 通常勤務
2 テレワーク 通常勤務
2 テレワーク 08:30-17:30
2 テレワーク 08:30-17:30
2 テレワーク 通常勤務
2 出社 08:00-17:00
2 テレワーク 通常勤務
2 テレワーク 通常勤務
2 出社 通常勤務
2 テレワーク 通常勤務
2 テレワーク 通常勤務
直近30日の状況
場所等 AMテレ... AM休 PMテレ... PM休 その他 テレワ... 出社 全休
160 140 120 100 80 60 40 20 0
41 42 5 5 43 43 5 46 50 11
77 50 70 62 6 59 67 59 72 5 59 63
25 26 27 30 31 1 2 3 4
March

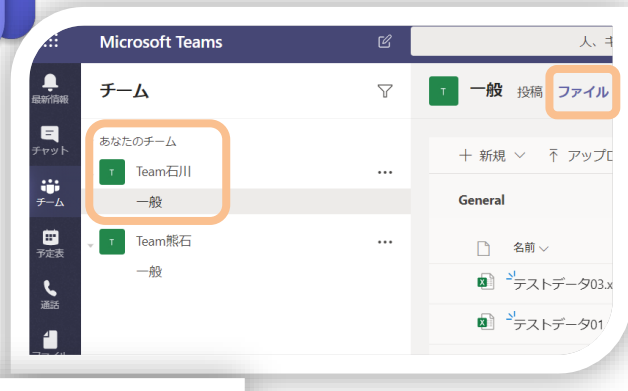
同じMicrosoft 365グループで利用

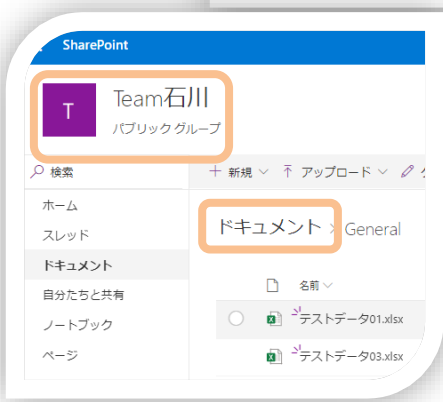
IDに紐づくグループで「ガバナンス」が効きやすい











貸与iPhoneの場合の主な考慮事項

02 デバイス管理

MDM/Intune

03 アクセスコンロール

条件付きアクセス

04 アプリケーション管理

MAM/Intune

貸与PCの場合

iPhoneより考慮事項が多くなる

貸与PCの場合

01 テナント構成

02 デバイス管理

03 アクセスコンロール

04 アプリケーション管理

05 外部ユーザー協業

06 セキュリティ強化

07 ガバナンス

08 コンプライアンス

09 監査

Azure AD Webinar(https://aka.ms/AzureAdWebiner)の8つ観点にコンプライアンスを追加し独自に整理

9つのAzure AD関連観点をふまえたゼロトラストの取り組みの概要

	Before	After（一部は既存環境併用 or 漸減）
01 テナント構成	AD（組織内、パスワード/指紋認証）	AD同期したAzure AD（組織内外、貸与iPhoneと2要素，リスクベース認証、パスワードレス、顔認証/Windows Hello）
02 デバイス管理	デスクトップPC＋リモート用ノートの2台，端末証明書，シンクラ的利用，マスター複製	MDM/Intune，Azure AD Join，Win10 Enterprise E5，デバイス保護/WD Device Guard，暗号化/BitLocker，リモートワイプ → ノート一本化へ
03 アクセスコントロール	VPN接続，Akamai EAA	条件付きアクセス ユーザ，場所，デバイス，アプリ，リアルタイムリスクチェック MD for Identity
04 アプリケーション管理	RDP，OneLogin(SSO,AD連携)	エンタープライズアプリケーション(SSO)，Apps on Azure AD
05 外部ユーザー協業	メール等で限定的	Azure AD B2B，外部も2要素化，Teamsゲストユーザー運用確立
06 セキュリティ強化	ファイルサーバ部暗号化，USB禁止，SSI社内端末管理，個別端末対策の組み合わせ，Web分離環境，MD for Office 365	MD for Endpoint(EDR)，端末がSecurity Center連携 Endpoint DLP，セキュリティベースライン，Secure Score，Security Posture，ハイジーン，脅威インテリジェンス
07 ガバナンス	権限ワークフロー，アカウント棚卸し/アカンサス	権限の付与・はく奪の効率化/自動化 情報保護/ラベル Information Protection & Governance
08 コンプライアンス	内部脅威検知/エルテスIRI等	Communication Compliance，Insider Risk Management，CASB/MDfCA，DLP(データ損出防止)，自動暗号化/検出，Zscaler等
09 監査	ログ定期分析，SIEM(Splunk ES)等	SIEM(既存 ＋ MS Sentinel試行)，原則ゼロトラストベース

Azure AD Webinar(https://aka.ms/AzureAdWebiner)の8つ観点にコンプライアンスを追加し独自に整理

MD：Microsoft Defender WD：Windows Defender

参考情報等

https://ishiayaya.net/win-security

https://www.fsa.go.jp/common/about/research/20210630.html

ゼロトラストとID強化に関する進め方のポイント

- 当初はシンプルに「大事な観点は何か」を考える
- 脱サイロ化：担当範囲を少し広げて柔軟に
- 自社にとって大事な観点に徐々に絞る(全部は不要)
- 3つのポイント(ID、EDR、共有)を念頭に
- 社内外の関係者とコミュニケーションを取りながら
- 勉強会（社外、社内）、動画、外部資料、SNS
- だんだんとわからなくなったら「当初」に戻る

ご静聴ありがとうございました。

be

agile