

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

ディスクレーム等

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 for Data Platform – Power BI Since Sep. 2021
- 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 になってみよう!」 #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



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

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」

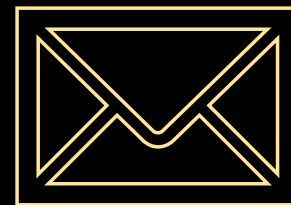
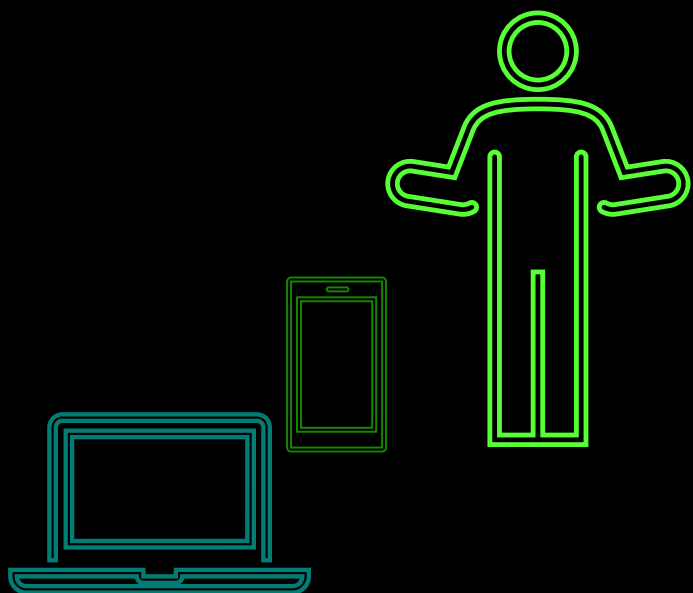
10大脅威 2021

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口 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

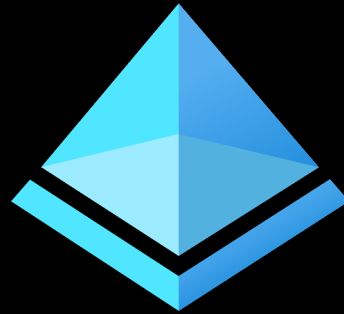
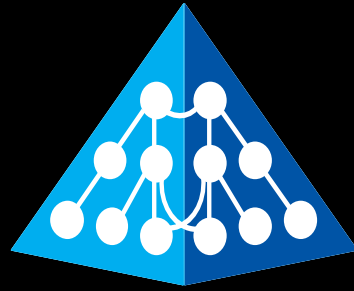
- 中から外部の接点である「Web」と「メール」が多い
- 境界防御は弱い中をガードする
- 中をモダンで高度にするのは難
- TLPT：中から

止めれば安全…



“人”等のIDをしっかりと、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つながら、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」をご紹介しますとともに、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

[受信登録の取り消し](#) | [プライバシーに関する声明](#) | [プライバシーに関するお問い合わせ](#)

日本マイクロソフト株式会社
〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー

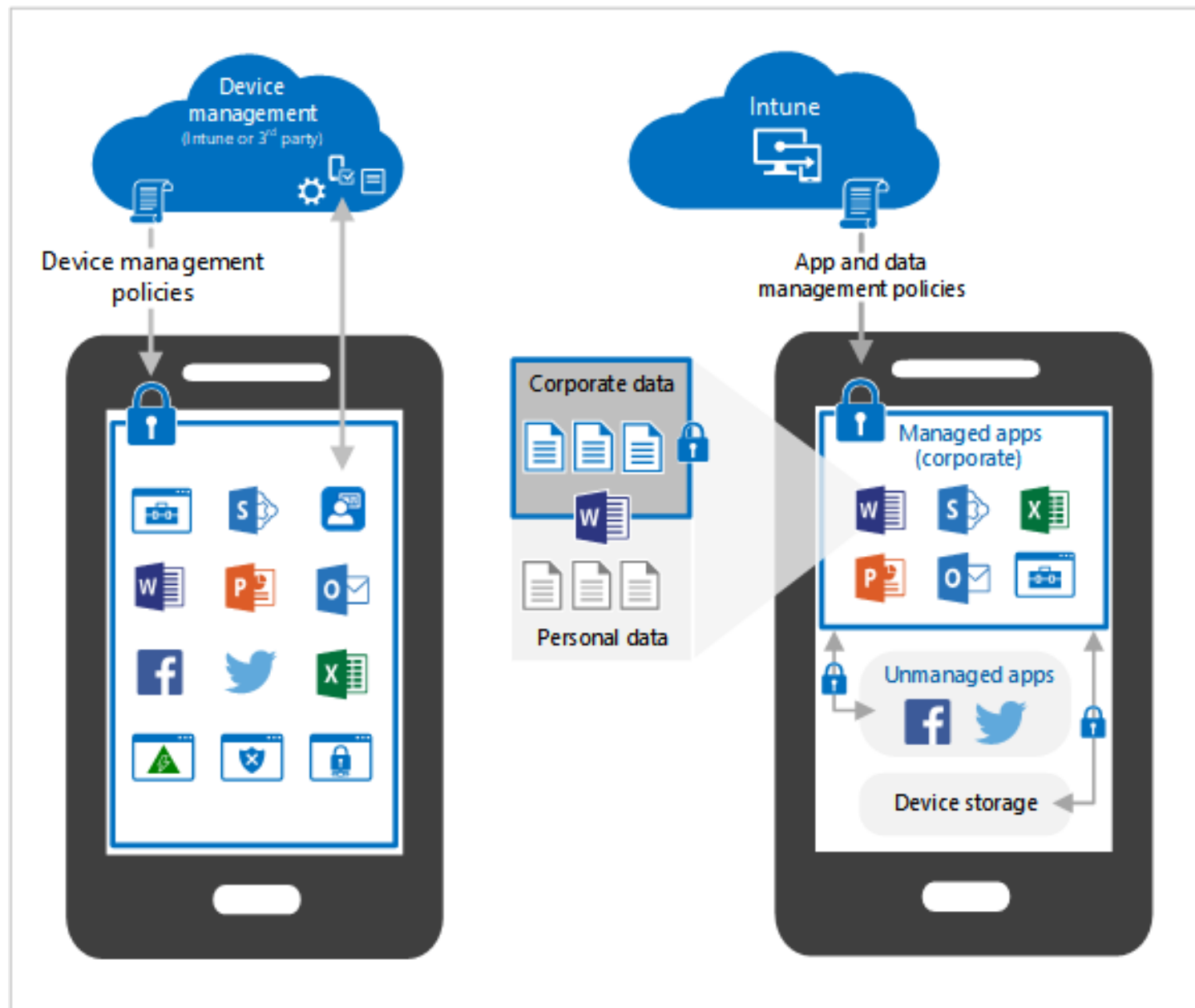
< メモ



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

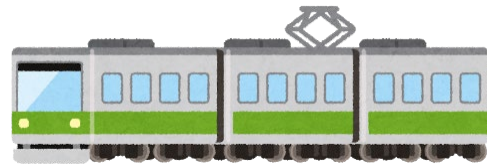


MAM

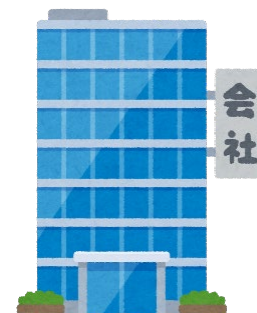
出所 「Microsoft Enterprise Mobility + Security (EMS) で BYOD を有効にするための技術の決定事項」 より一部抜粋
<https://docs.microsoft.com/ja-jp/intune/fundamentals/byod-technology-decisions>

急にきたコロナ禍

ビフォーコロナ



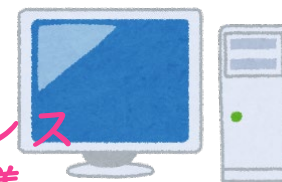
コロナ禍



Microsoft 365



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



ゼロトラストで
リアルでいろんなチェックがあるけど
ダイレクトに

Microsoft 365



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>



<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」「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 Decode 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かっちりできている企業はどれく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リギ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

AzureAD Japan
チャンネル登録者数 646人

ホーム 動画 再生リスト チャンネル プリートーク 概要

アップロード済み すべて再生

並べ替え

5-6: マイクロソフト サポート部門が送る 「Azure AD ... 757 回視聴・3 か月前

5-5: インフラ担当者のための Azure AD 開発入門 464 回視聴・4 か月前

5-4: [実装編] あなたの資産をちゃんと管理できています... 202 回視聴・4 か月前

5-3: [解説編] あなたの資産をちゃんと管理できています... 354 回視聴・5 か月前

5-2: Goodbye ADFS 2021 564 回視聴・5 か月前

5-1: オンプレ AD から Azure AD への移行計画 ~ 「今何... 1458 回視聴・6 か月前

4-6: マイクロソフトサポート部門が送る 「よくある... 675 回視聴・11 か月前

4-5: COVID-19 でリモート対応に成功した企業と失敗し... 401 回視聴・11 か月前

4-4: オンプレミス アプリケーションのモダン化 452 回視聴・11 か月前

4-3: パスワードレス (後編) - パスワードレス導入方法論 463 回視聴・11 か月前

4-2: パスワードレス (前編) - パスワードレスの価値と任... 870 回視聴・11 か月前

4-1: Azure AD アーキテクチャ概要 - Azure AD を設計... 1375 回視聴・11 か月前

3-6: Hybrid Azure AD Join 動作の仕組みを徹底解説 1343 回視聴・11 か月前

3-5: Intuneによるモバイルデバイスとアプリのセキュア... 2054 回視聴・11 か月前

3-4: Azure AD の新しいデバイス管理パターンを理解し... 860 回視聴・11 か月前

3-3: 詳説! Azure AD 条件付きアクセス - 設計のやり方編 844 回視聴・11 か月前

3-2: 詳説! Azure AD 条件付きアクセス - 動作の仕組み... 1358 回視聴・11 か月前

3-1: モダンアクセスコントロール実現に向けた戦略策定... 615 回視聴・11 か月前

2-5: Azure AD で実現する SaaS 外部パートナー協業 233 回視聴・11 か月前

2-4: Azure AD の SaaS アプリケーション認証への活用 640 回視聴・11 か月前

2-3: Office365 および Azure AD 管理者が必ずやってお... 397 回視聴・11 か月前

2-2: IP ベースのアクセス制御からの脱却してよりセキ... 511 回視聴・11 か月前

2-1: Azure Active Directory 利用開始への第一歩 1466 回視聴・11 か月前

1-5: Azure AD セルフサービス機能を有効活用する方法 433 回視聴・11 か月前

1-3: Office365 および Azure AD 管理者が必ずやってお... 1136 回視聴・11 か月前

1-1: 適切な Azure AD 認証方式の選択の決め手 2100 回視聴・11 か月前

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

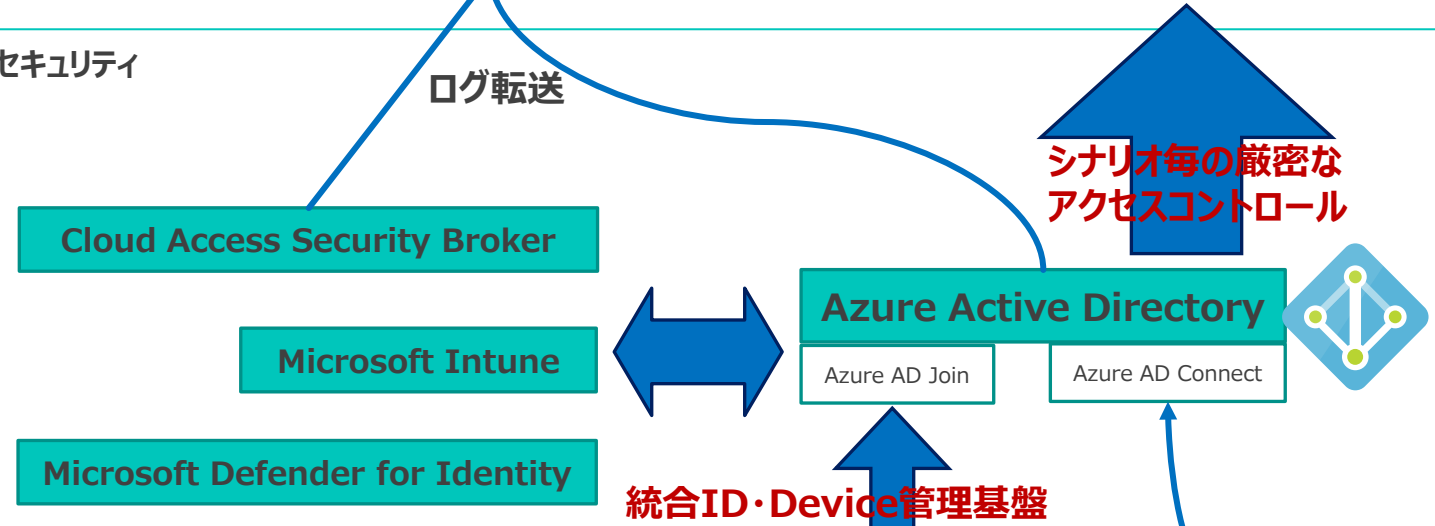
グラウンドデザイン

* 一部試行等含む

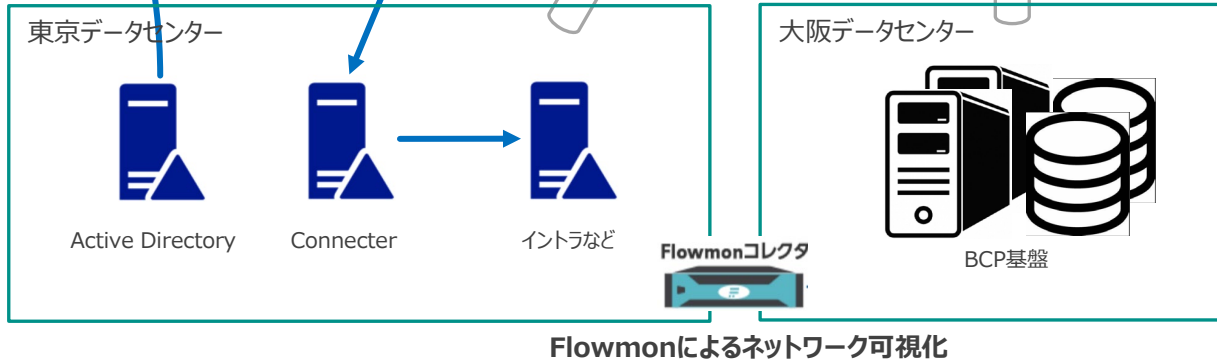
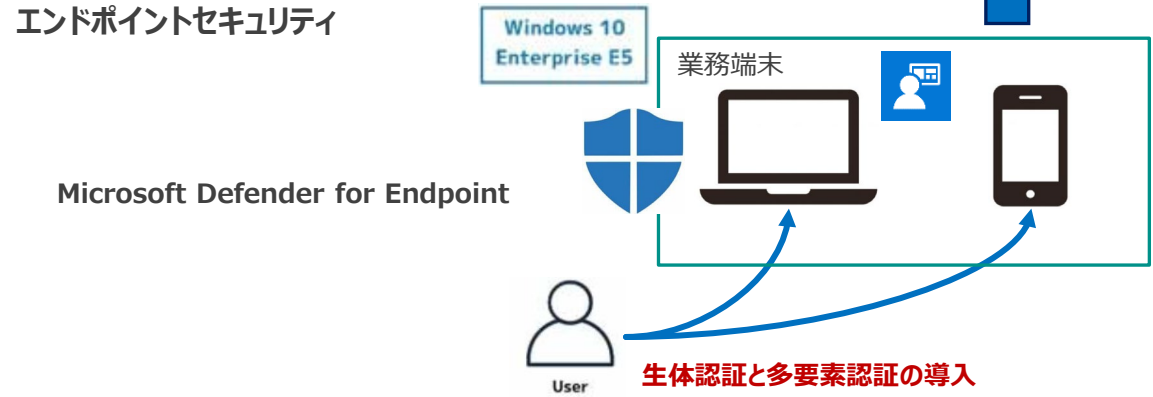
その他クラウドサービス



クラウドセキュリティ



エンドポイントセキュリティ



Flowmonによるネットワーク可視化

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

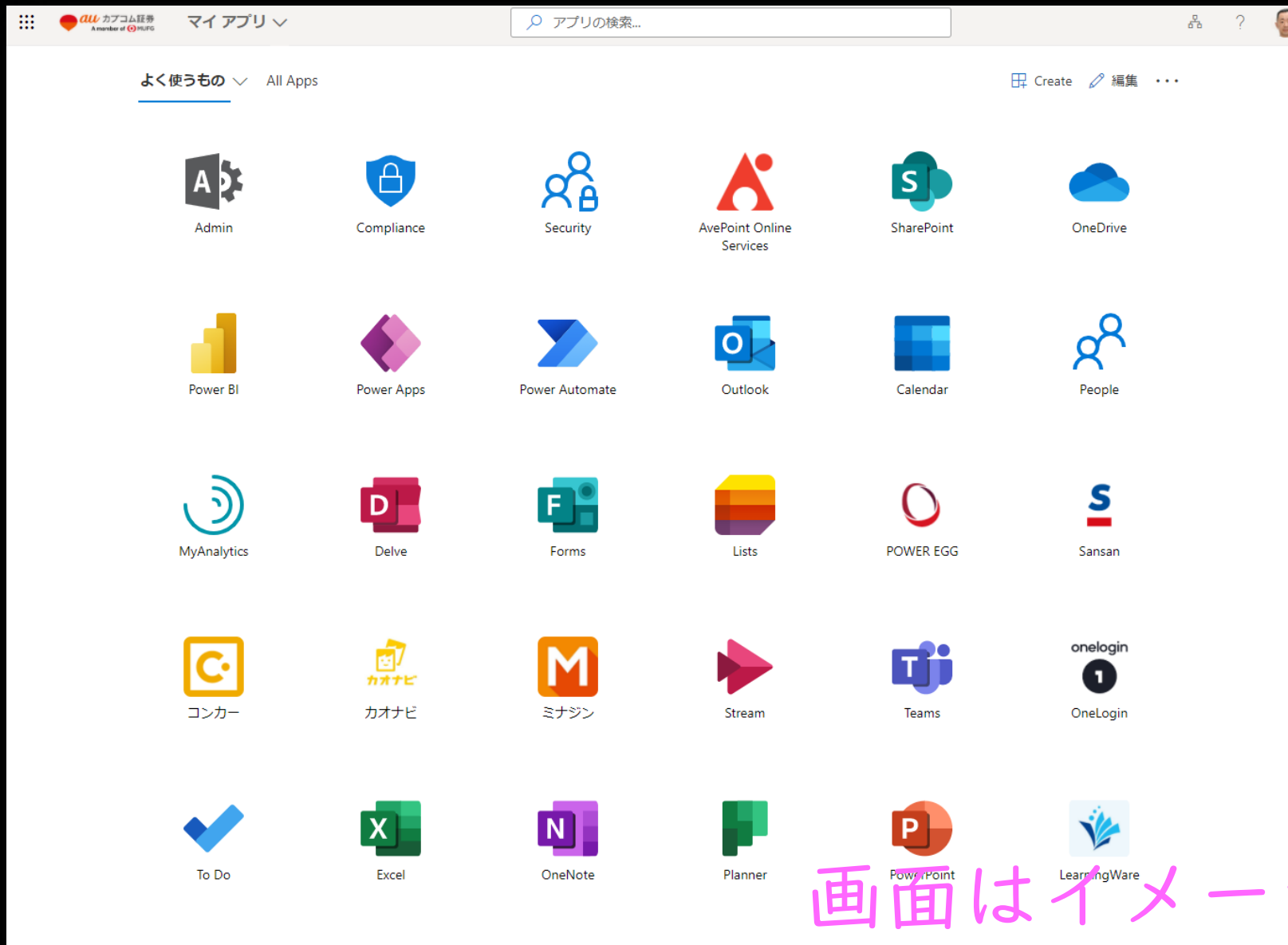


- パスワード → 多要素 →
パスワードレス



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

Azure Active Directory 管理センター

ダッシュボード > 石川陽一 > セキュリティ > 条件付きアクセス >

Office 365 & Power BI Session Control

条件付きアクセス ポリシー

削除

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてユーザー アクセスを制御します。 [詳細情報](#)

名前 *

Office 365 & Power BI Session Control

割り当て

ユーザーとグループ ①

すべてのユーザー

クラウド アプリまたは操作 ①

3 個のアプリ 件を含む

条件 ①

2 個の条件が選択されました

アクセス制御

許可 ①

1 個のコントロールが選択されました

セッション ①

アプリの条件付きアクセス制御を使う

リスク、デバイス プラットフォーム、場所、クライアント アプリ、またはデバイスの状態などの条件からのシグナルに基づいて、ユーザー アクセスを制御します。 [詳細情報](#)

ユーザーのリスク ①

未構成

サインインのリスク ①

未構成

デバイス プラットフォーム ①

未構成

場所 ①

未構成

クライアント アプリ ①

1 件を含む

デバイスの状態 (プレビュー) ①

すべてのデバイスの状態

デバイスのフィルター (プレビュー) ①

未構成



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



- 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

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

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

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

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

セキュリティ ニュース フィード

Microsoft 365 Defender

A Twitter list by @MeffSecIntel
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...

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...

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

画面はイメージです

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...

Incidents > Unsanctioned cloud app... > **Unsanctioned cloud app access was blocked**

Unsanctioned cloud app access was blocked

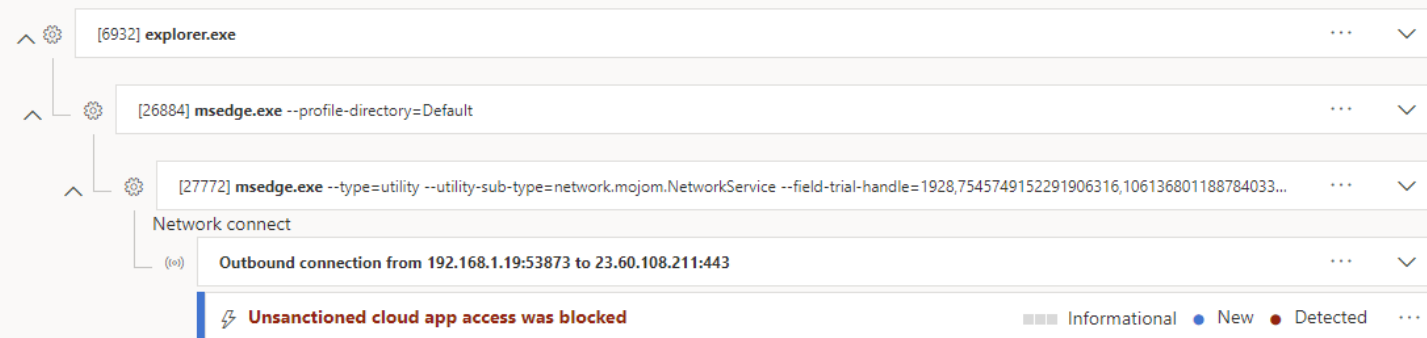
ishidesktop2021 Risk level Informational

azuread\ishiyaya

Data sensitivity:機密

ALERT STORY

Expand all



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

The screenshot displays the Microsoft Azure Sentinel dashboard. At the top, there's a navigation bar with the Microsoft Azure logo and the user's name 'ishiayaya@ishiayaya.info'. Below this, the dashboard title is 'Azure Sentinel | 概要' (Overview). The main content area is divided into several sections:

- Summary (概要):** Shows a total of 1,100 events (1.1千) with a green upward arrow and 598 alerts (598). It also indicates 0 warnings (警告) and 0 incidents (インシデント).
- Incident Status (状態別インシデント):** Shows 0 new incidents (新規), 0 active incidents (アクティブ), and 0 resolved incidents (解決済み).
- Time-based Events and Alerts (時間経過に伴うイベントとアラート):** A bar chart showing event counts over time. The Y-axis ranges from 0 to 180. The X-axis shows times: 12時, 18時, 8月23日, and 6時. A legend on the right lists: ALERTS (0), OFFICEACTIVITY (744), SIGNINLOGS (206), INFORMATION... (58), and OTHERS (2) (60).
- Alerts (警告):** A section with a 'データが見つかりませんでした' (Data not found) message.
- Data Source Anomalies (データソースの異常):** A line chart showing OfficeActivity anomalies over time. The Y-axis ranges from 0 to 10. The X-axis shows times: 12時, 18時, 8月23日, and 6時.
- Events with Potential Malicious Intent (悪意のある可能性があるイベント):** A map showing the geographical distribution of events. A legend indicates 0 events with potential malicious intent (悪意のある可能性があるイベント).

画面はイメージです



Azure Sentinel | ハンティング

選択したワークスペース: 'sentinel-ishiyaya'

検索 (Ctrl+/) << 最新の情報に更新 過去 24 時間 | 新しいクエリ 全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

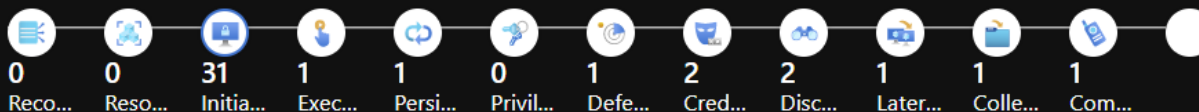
- ノートブック
- エンティティの動作
- 脅威インテリジェンス (プレビュー)

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



クエリの検索 方針: Initial Access フィルターの追加

<input type="checkbox"/>	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...
<input type="checkbox"/>	★ Failed Login Attempt by Expi...	Microsoft	SecurityEvent +1 ⓘ	--	--
<input type="checkbox"/>	★ Multiple Password Reset by ...	Microsoft	AuditLogs +3 ⓘ	--	--
<input type="checkbox"/>	★ Rare domains seen in Cloud ...	Microsoft	AuditLogs +2 ⓘ	--	--
<input type="checkbox"/>	★ Exploit and Pentest Framew...	Microsoft	W3CIISLog +2 ⓘ	--	--
<input type="checkbox"/>	★ Anomalous sign-in location ...	Microsoft	SigninLogs	--	--
<input type="checkbox"/>	★ Attempts to sign in to disabl...	Microsoft	SigninLogs	--	--
<input type="checkbox"/>	★ Attempts to sign in to disabl...	Microsoft	SigninLogs	--	--
<input type="checkbox"/>	★ Inactive or new account sign...	Microsoft	AuditLogs +1 ⓘ	--	--
<input type="checkbox"/>	★ Login attempts using Legacy...	Microsoft	SigninLogs	--	--
<input type="checkbox"/>	★ Failed attempt to access Azu...	Microsoft	SigninLogs	--	--
<input type="checkbox"/>	★ Anomalous Azure Active Dir...	Microsoft	SigninLogs	--	--
<input type="checkbox"/>	★ Azure Active Directory signi...	Microsoft	SigninLogs	--	--

画面はイメージです

見える化



@ishiyaya.inf
- (ISHIAYAYA.INFO

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 Information Protection (プレビュー) >

ログ Sentinel-ishiyaya

新しいクエリ 1*

Sentinel-ishiyaya

実行 時間の範囲: カスタム 保存 共有 新しいアラートルール

エクスポート

- CSV ヘクスポート - すべての列
- CSV ヘクスポート - 表示されている列
- Power BI ヘクスポート (M Query)
- Excel で開く

テーブル クエリ 関数

検索

フィルター グループ化の基...

すべて折りたたむ

お気に入り

お気に入りを追加するには、次をクリックします: ☆ アイコン

Azure Sentinel

LogManagement

カスタム ログ

```
1 InformationProtectionLogs_CL
2 | summarize count() by Operation_s, TimeGenerated
3 | sort by TimeGenerated
```

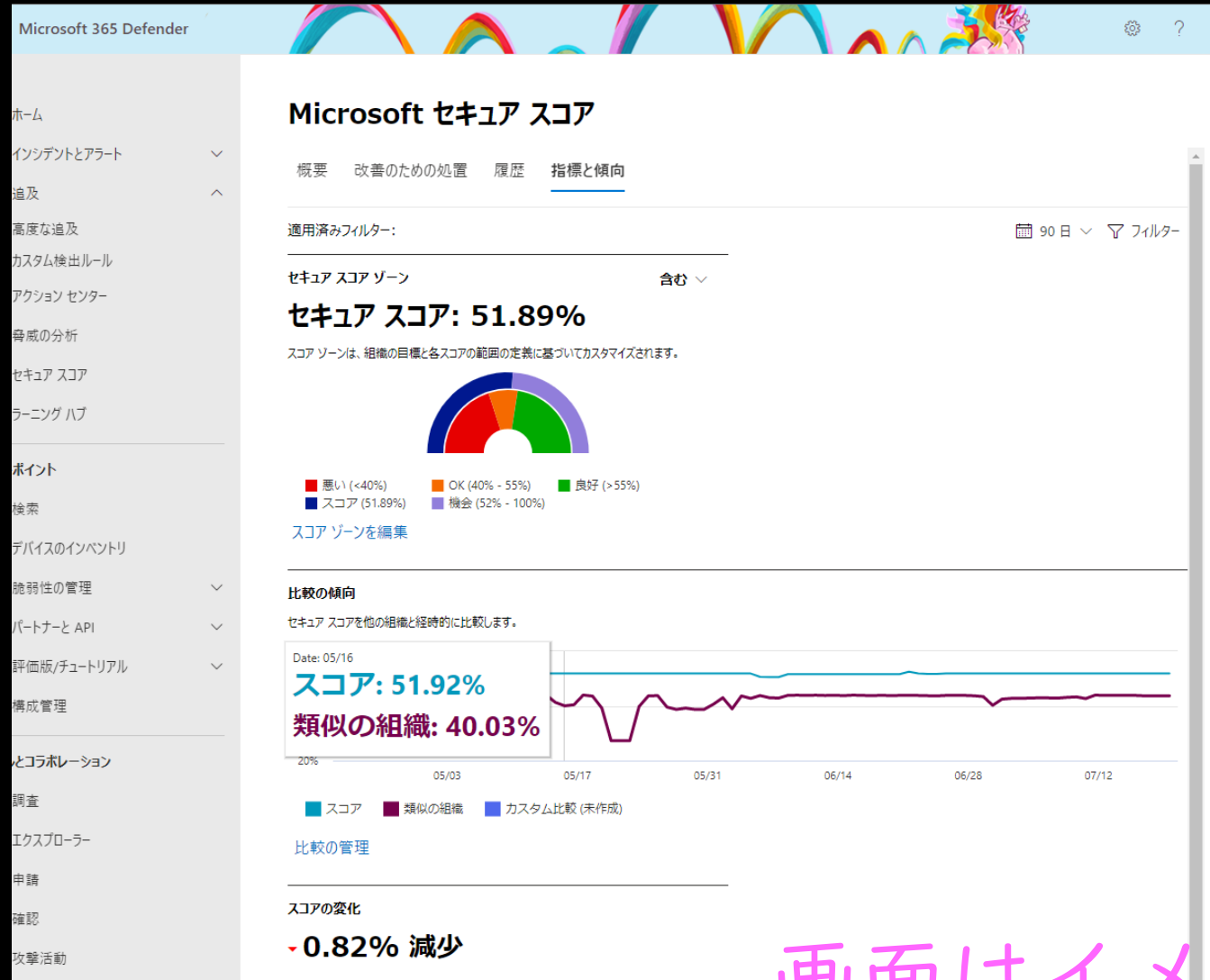
結果 グラフ 列 ブックマークの追加 時刻の表示 (UTC+09:00) 列のグループ化

完了. カスタムの時間範囲 からの結果を表示しています。 00:00.6 383 個のレコード

TimeGenerated [大阪、札幌、東京]	Operation_s	count_
> 2021/8/23 9:01:03.166	Discover	1
> 2021/8/23 9:01:03.149	Heartbeat	1

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



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



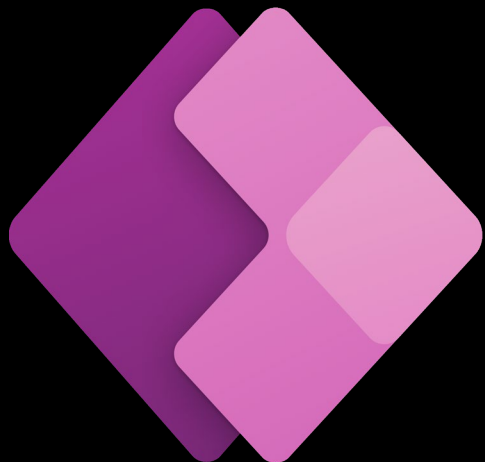
2020/03/31

出社
07:30-16:30



2020/03/26

テレワーク
06:00-15:00



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

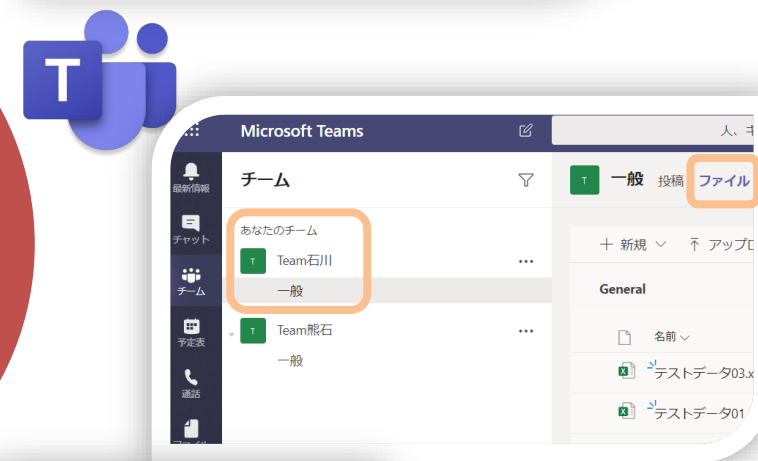
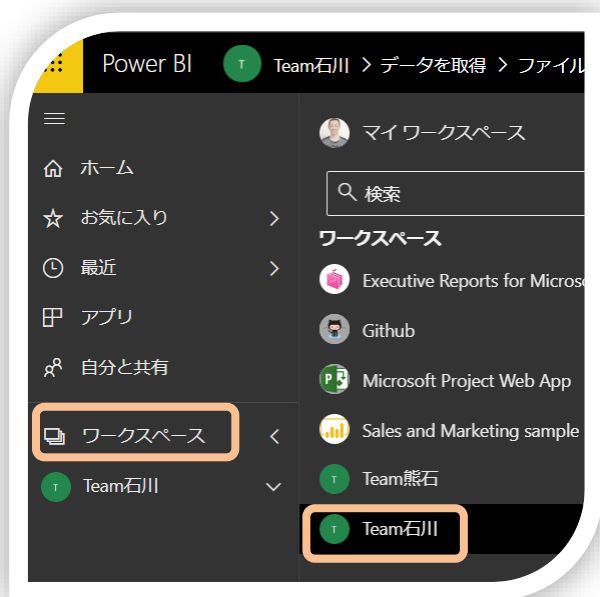
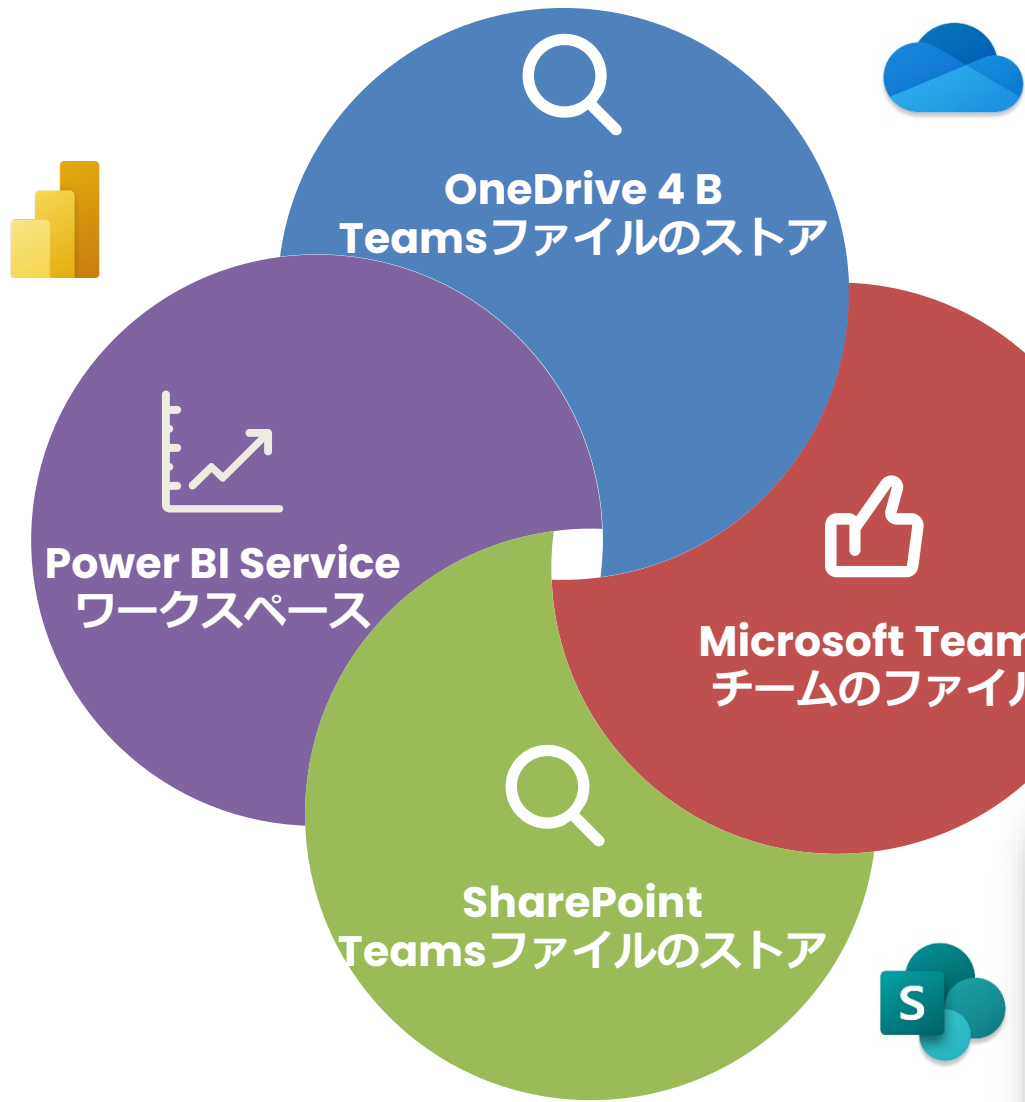
	ステータス	起案期限	起案日
企画概要	相談済み	-----	2020/08/06
エントリー票	承認済み	2020/08/05	2020/08/06
プロジェクト承認書	承認未済	2020/08/05	

案件情報

案件番号	案件種別	管理 LV
20-029	制度改正	
案件名		

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



貸与PCの場合

iPhoneより考慮事項が多くなる

貸与PCの場合



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

01 デナント構成
AD (組織内、パスワード/指紋認証)

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

03 アクセス
コントロール
VPN接続, Akamai EAA

04 アプリケーション
管理
RDP, OneLogin(SSO,AD連携)

05 外部ユーザー
協業
メール等で限定的

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

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

08 コンプライアンス
内部脅威検知/エルテスIRI等

09 監査
ログ定期分析, SIEM(Splunk ES)等

After (一部は既存環境併用 or 漸減)

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)

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

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

エンタープライズアプリケーション(SSO), Apps on Azure AD

Azure AD B2B, 外部も2要素化, Teamsゲストユーザー運用確立

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

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

Communication Compliance, Insider Risk Management,
CASB/MDfCA, DLP(データ損出防止), 自動暗号化/検出,
Zscaler等

SIEM(既存 + MS Sentinel試行), 原則ゼロトラストベース

MD : Microsoft Defender WD : Windows Defender



参考情報等



10



13



...

@ishiyaya が2021年09月06日に更新 3672 views

Azure AD & Windows Security等メモ

セキュリティ, Windows10, AzureActiveDirectory, AzureAD, Microsoft365



はじめに

Azure AD Webinar (<https://aka.ms/AzureAdWebiner>) Season4-1 (8項目) +コンプラを軸にde:code2020のセキュリティセッションでクローズアップされたキーワード等を独自にマッピングしてみました。

[2021/09/06更新] Azure AD Webinar Seasonに関するメモ

- 過去分は資料 (PPT等) はGitHubから取得できます。
- Season 1~5は全て、原則録画がYouTubeで視聴できます。
- 以下、タイトル、カッコは私見のキーワード、重複するセッションの除外等のメモです。

Season 1 (2018年 5月 - 7月実施)

- #1 適切な Azure AD 認証方式の選択の決め手 (パスワードハッシュ同期一択)
- #5 Azure AD セルフサービス機能を用いてコスト削減
- #2~#4は、一部動画再生がNGだが、Season 2の#3~#5と順番は違えど同テーマなのでそちらを参照

<https://ishiyaya.net/win-security>

ホーム

金融庁について

お知らせ・広報

政策・審議会等

法令・指針等

アクセスFSA
(金融庁広報誌)

[ホーム](#) > [金融庁について](#) > [金融庁について](#) > [委託調査・研究等](#)

令和3年6月30日
金融庁

「ゼロトラストの現状調査と事例分析に関する調査報告書」 の公表について

金融庁では、これまで官民が一体となって金融分野のサイバーセキュリティ強化に取り組んで参りました。こうした中、サイバー攻撃は引き続き複雑化・巧妙化しており、更なるサイバーセキュリティ強化に取り組んでいく必要があると見ています。

デジタル化の進展に伴い、金融機関においても、クラウドの利用や外部委託先とのデータ連携等が進み、従来の境界防御ではなく、侵入されることを前提としたセキュリティ対策が注目されています。

ゼロトラストとは、こうしたデジタル化を踏まえ、ネットワークの内外にかかわらず、従業員の端末通信や情報資産へのアクセス等についても常に監視することでセキュリティを確保する考え方です。

この度、金融機関によるセキュリティ対策の促進及びモニタリングの参考等に活用するため、ゼロトラストの現状と事例分析に関する調査について、PwCあらた有限責任監査法人に委託し、報告書として取りまとめました。

報告書については、別添PDFをご覧ください。

(別添)  [ゼロトラストの現状調査と事例分析に関する調査報告書 \(PDF: 2,131KB\)](#)

<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