#shifthappens

auカブコム証券、「ゼロトラスト」への挑戦 - Microsoft 365 利活用と情報漏洩対策

auカブコム証券株式会社
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
可能性があります。

石川 陽一 @ishiayaya

- 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
- 今年からコミュニティを開始
  「市民開発者 なってみよう!」 #TryCivicEngr

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 5ヶ月で-30kg ダイエット(2019 半戻し状態から1ヶ月で-10kg)

2015 半年で3回致死的不整脈。ICD装着。身障1級

2013 システム監査・内部監査

2017/2- サイバー等セキュリティ

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

会社概要

- 2019/12/2 商号変更
- 口座数 約127万口座
- 従業員数 約177名
- 拠点数 2→1

本日のアジェンダ

1 DXとゼロトラスト、これまでの取り組み

2 あの心配ごとと向かい合う

3 なぜPIか

IDXとゼロトラスト、これまでの取り組み

#shifthappens

2017年のDX取り組み開始前後～

2017～

働き方改革

- 情報共有が弱い
- ダッシュボードがない
- 社内ITが弱い
- 紙、押印、進展しないGW
- ID管理が雑
- メールが多い
- どこか人力感
  ＝コミュニケーションが部分的に×
- IT部門以外もITを迅速に使えないと

デジタルトランスフォーメーションを支えるIT主導の働き方改革

～ クラウド+テレワークで生産性向上を推進。 仮想PBXに対応したau iPhoneを活用 ～

2017年6月22日 お知らせ

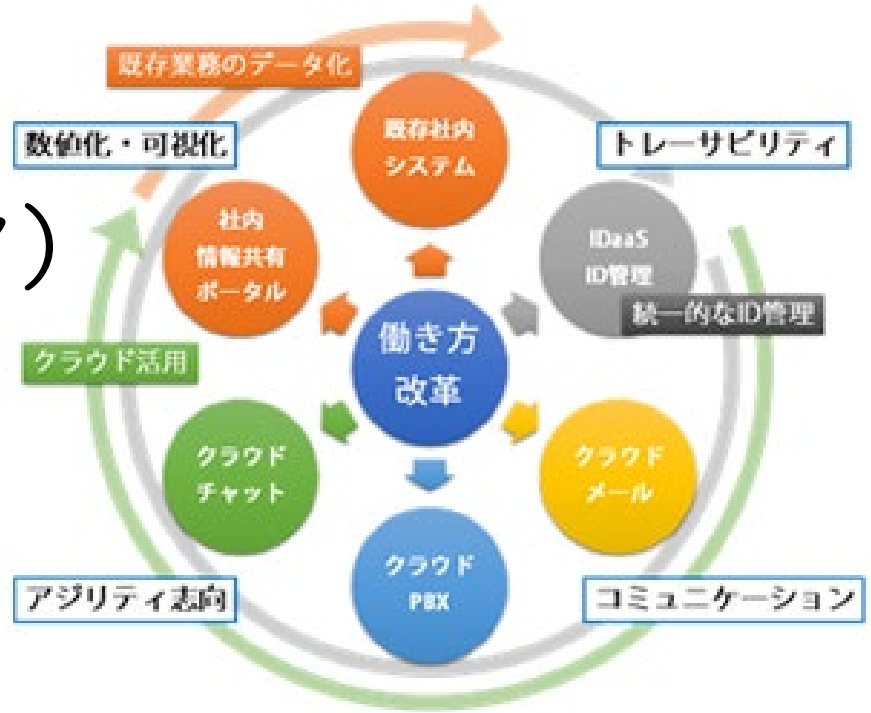
カブドットコム証券株式会社（代表執行役社長：齋藤 正勝、証券コード：8703、以下「当社」）は、「デジタルトランスフォーメーションを後押しする抜本的な働き方改革」をテーマとし、「クラウドとテレワークを活用したIT主導での生産性向上」を目指す社内業務改革の取り組みを開始しました。

当社は、社内業務におけるコミュニケーション・プラットフォームの刷新を中心に、積極的にクラウド基盤やクラウドサービスを活用し、社内外の業務効率向上のための改革を進めます。各種最新デバイスを活用しテレワーク（リモートワーク）環境を拡充、業務のデジタル化・自動化による生産性の向上を推進し、業務改革としてデジタルトランスフォーメーションを軸足とした働き方改革により、企業価値の一層の向上と上場企業としての社会的責任を果たし、実践して参ります。

デジタルトランスフォーメーションを支えるIT主導の働き方改革

～ クラウド+テレワークで生産性向上を推進。 仮想PBXに対応したau iPhoneを活用 ～

- クラウドPBX+内線iPhone(MDM)
- ビジネスチャット
- Win10Ent + O365
- POWER EGG（新グループウェア）
- IDaaS
- 情報の可視化



2017～2018頃

働き方改革

- 情報共有が弱い
- ダッシュボードがない
- 社内ITが弱い
- 紙、押印、進展しないGW
- ID管理が雑
- メールが多い
- どこか人力感
  ＝コミュニケーションが部分的に×
- IT部門以外もITを迅速に使えないと

（2019年春）貸与iPhoneの場合

「iPhoneで予定も見られないの？…」

一定のセキュリティがあれば、便利なことを使える

「現状よりも、よりよくしたい」

- 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…

2020/2/27 危機管理対策本部

既存の危機管理チーム上に設置

00 2020新型コロナウイルス対応
OP_BCP危機対策本部

一般

ここまではよかったのですが…

感染症対応に伴う各部室の業務運営体制管理（テレワーク・時差出勤利用状況一覧）

社員区分	部室	Gr	氏名	2月27日（木）		2月28日（金）		3月2日（月）		3月3日（火）		3月4日（水）		3月5日（木）		3月6日（金）	
就業形態	所属	所属2	従業員名	テレワーク	時差出勤	テレワーク	時差出勤	テレワーク	時差出勤	テレワーク	時差出勤	テレワーク	時差出勤	テレワーク	時差出勤	テレワーク	時差出勤
			利用人数	26	36	39	37	35	60	58	56	68	53	64	55	73	57
正社員	システム	部	F														
正社員	システム	部	F														
正社員	システム	部	F														
正社員	システム	部	F														
正社員	システム	部	F														
正社員	システム	部	F														
派遣社員	システム	部	F														
正社員	システム	部															
正社員	システム	部															
正社員	システム	部															
正社員	システム	部															
正社員	システム	部															

予定をExcelに入力するんだ
200人共有でバーン！

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

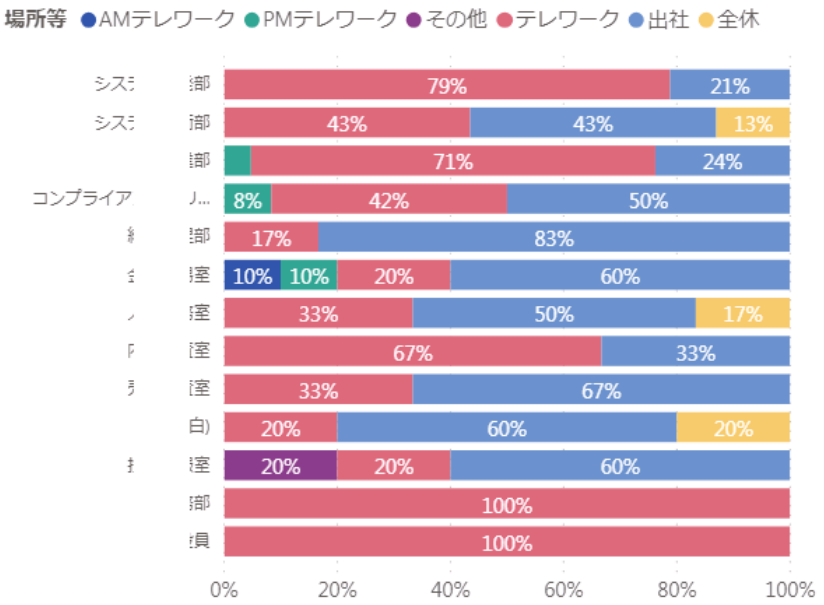
場所等
テレワーク

時差出勤
07:30-16:30

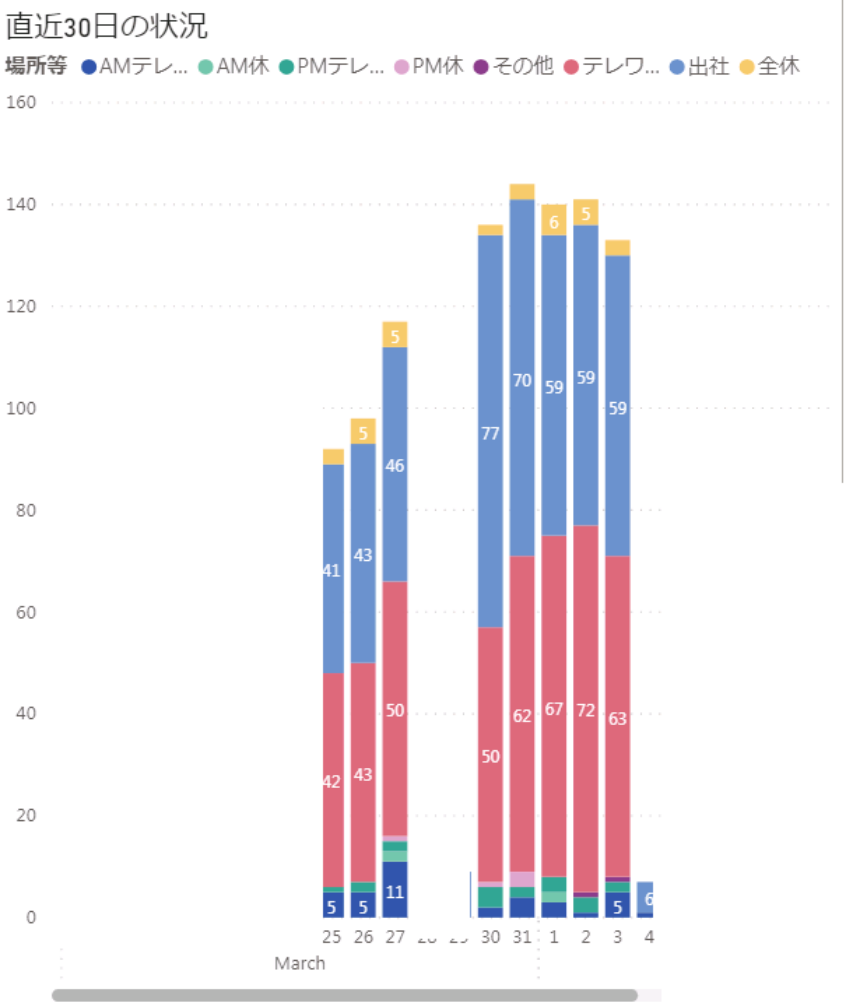
テレワーク・時差出勤 登録状況 簡易版

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



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

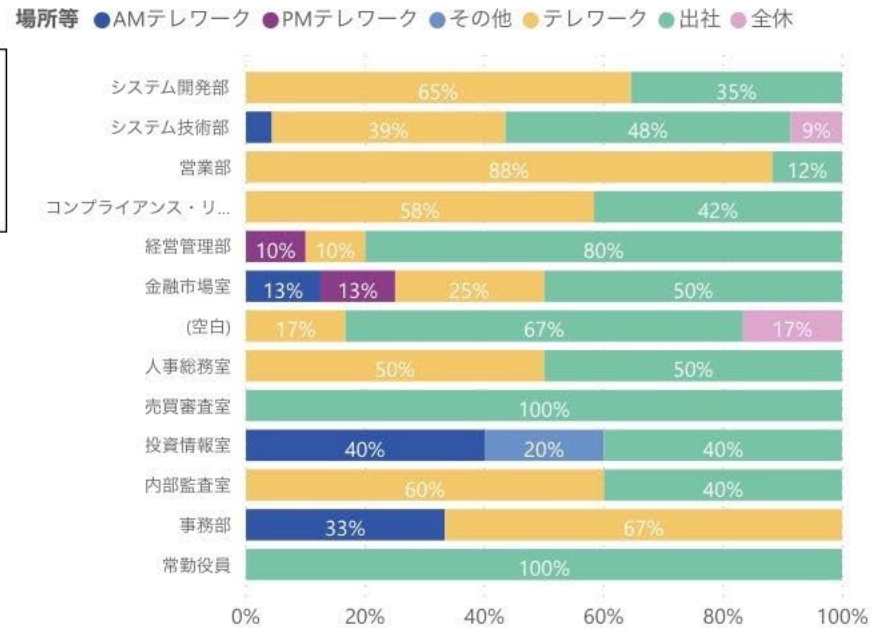


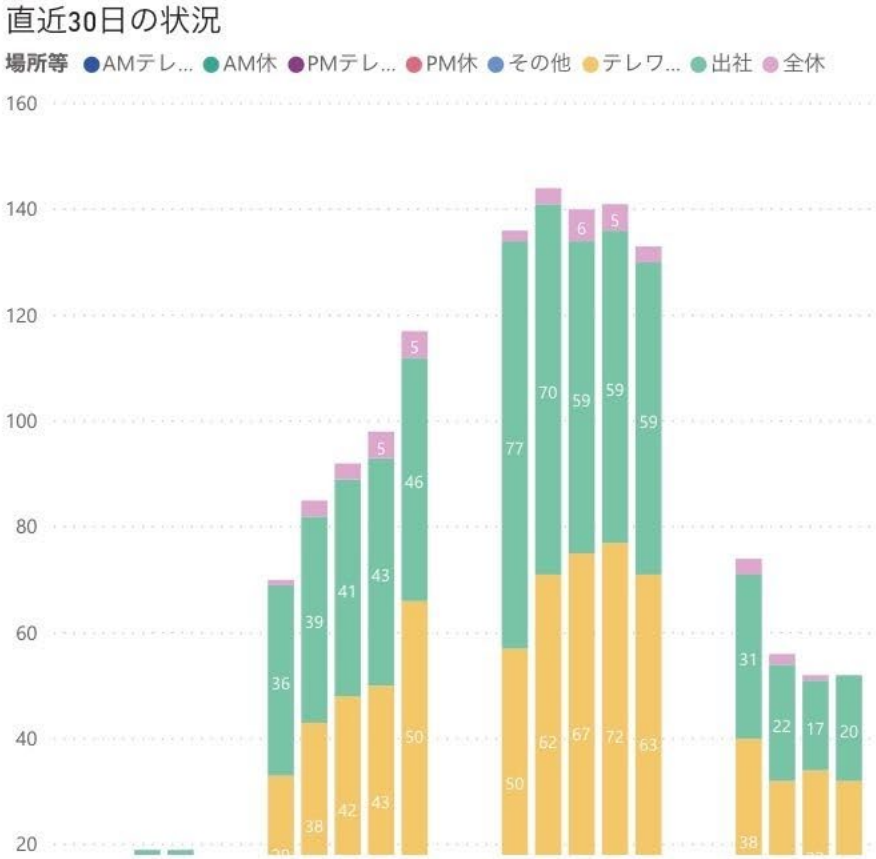
テレワーク等管理

テレワーク・時差出勤 登録状況 簡易版

69
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





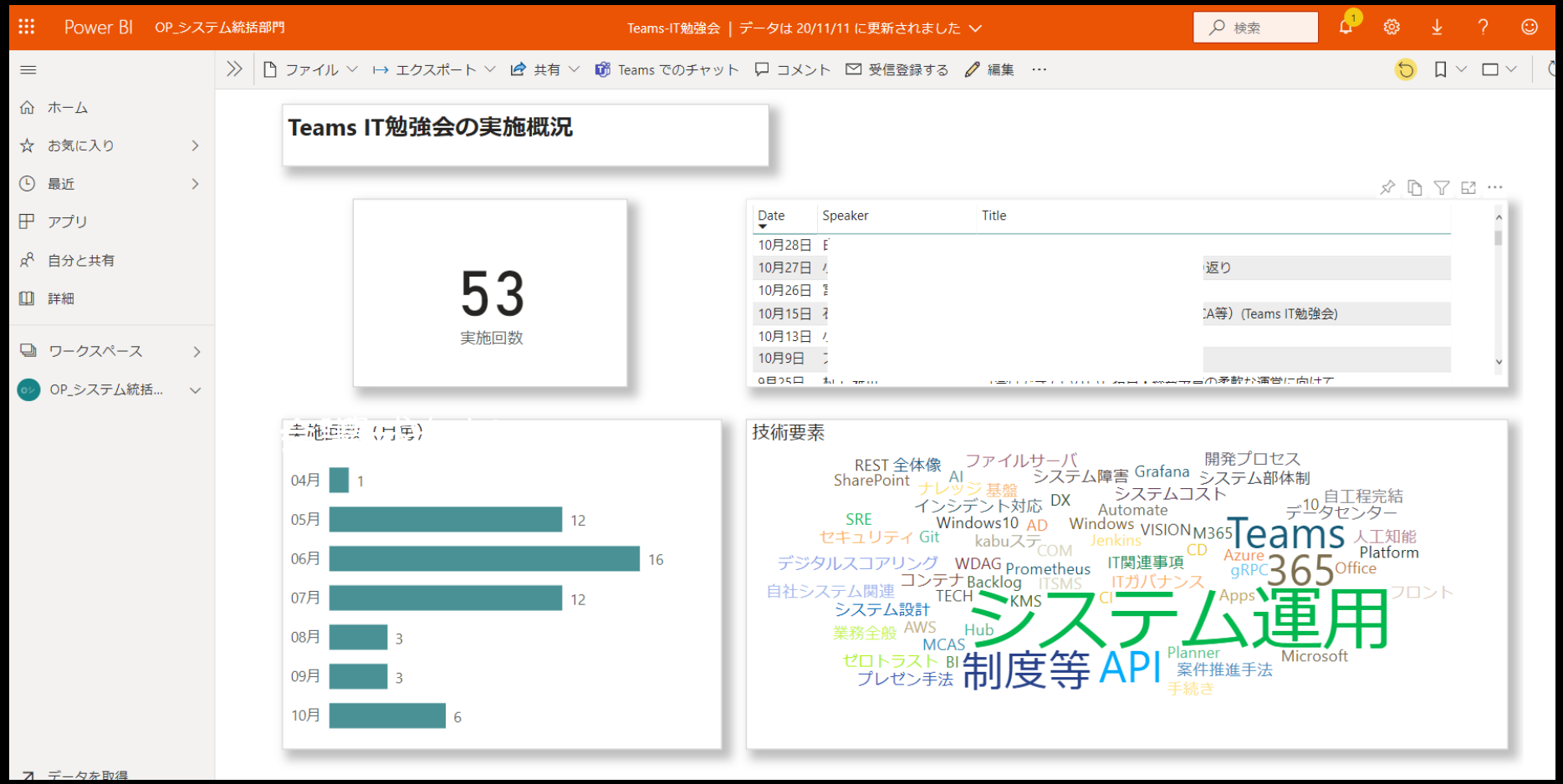
日	名前	Gr	場所等	時差出勤
3			テレワーク	09:00-18:00
3		フロント2グループ	テレワーク	08:30-17:30
3			テレワーク	08:30-17:30
3		企画グループ	出社	08:00-17:00
3		システムリスク管理グループ	テレワーク	通常勤務

ローコードアプリ展開


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

ランチタイムに社内IT勉強会



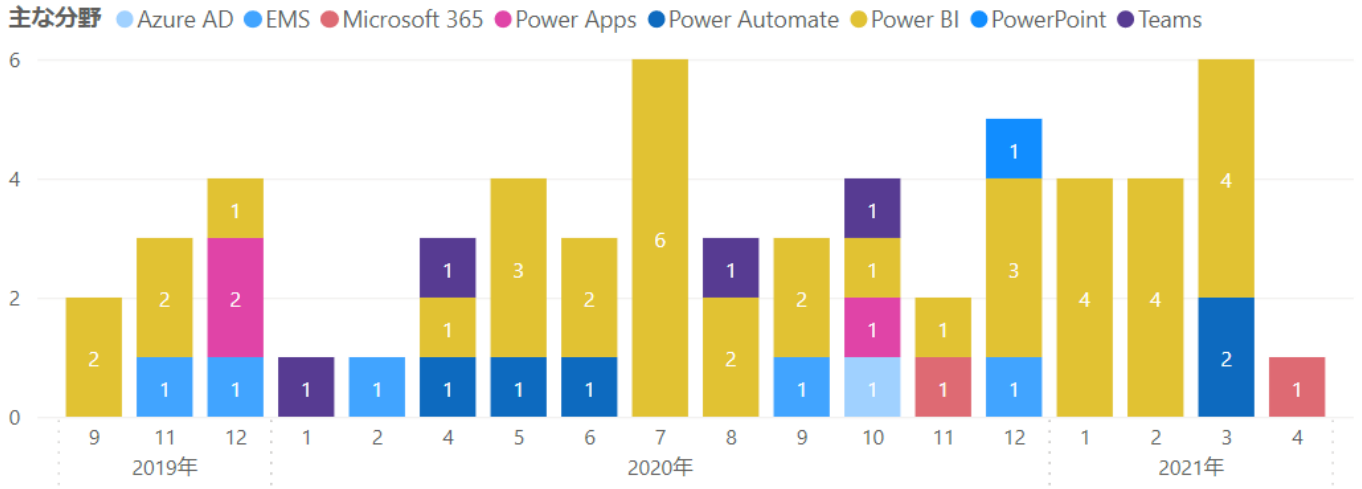
石川陽一 2020年の登壇等

https://ishiayaya.net/Talk

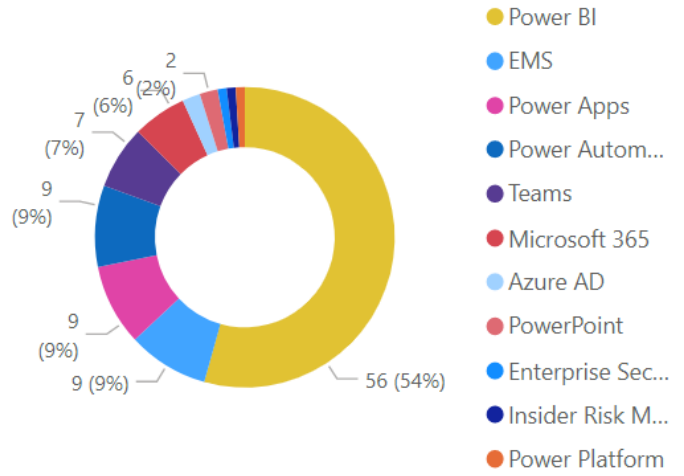
35
2020年の登壇回数

15
2021年の登壇回数

月毎の推移



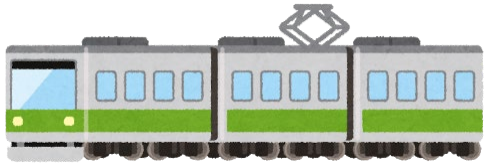
関連分野



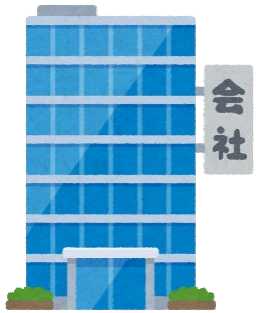
Date	活動	主な貢献分野	その他の貢献分野
2021/04/22	AvePoint #ShiftHappens 登壇 セキュリティ関連	Microsoft 365	EMS
2021/03/28	Power Automate Desktop勉強会 vol.2 LT 「Power Automate DesktopでPDF関係やってみた」	Power Automate	Power BI
2021/03/28	市民開発者 なってみよう! #5 自コミュニティ 「軽いPower Automate」	Power Automate	Power BI
2021/03/27	日本を元気に・革新コンソーシアム [第1回 現場改善会議]	Power BI	Microsoft 365
2021/03/18	JNSA｜Network Security Forum 2021 （NSF2021） 登壇 「2017年からのDXの取り組みと現在地、これから」	Power BI	Microsoft 365
2021/03/09	ビジネス+IT セキュリティマネジメントカンファレンス 2021 冬 登壇 「auカブコム証券のゼロトラストセキュリティへの取り組み」	Power BI	Microsoft 365
2021/03/06	Power BI 勉強会 #20 登壇 「Power BI最近試した3つ「DAX.doスマホ画面とアプリMIP & MCAS」」	Power BI	EMS

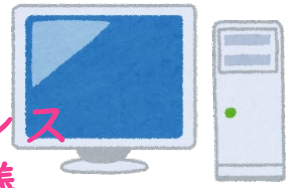
ゼロトラスト

ビフォーコロナ



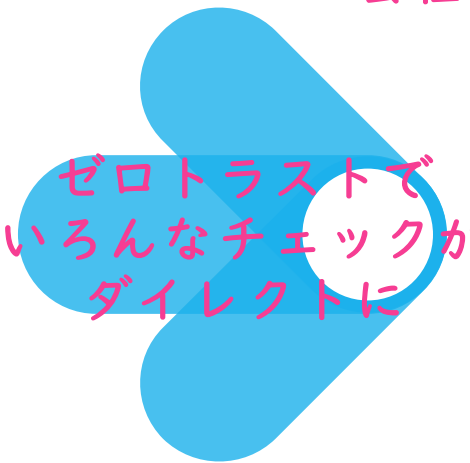
コロナ禍



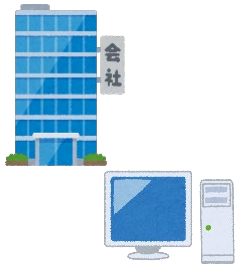


会議室ガラガラ
ソーシャルディスタンス
会社でもネット会議

Withコロナ



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



E5系の新環境

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

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

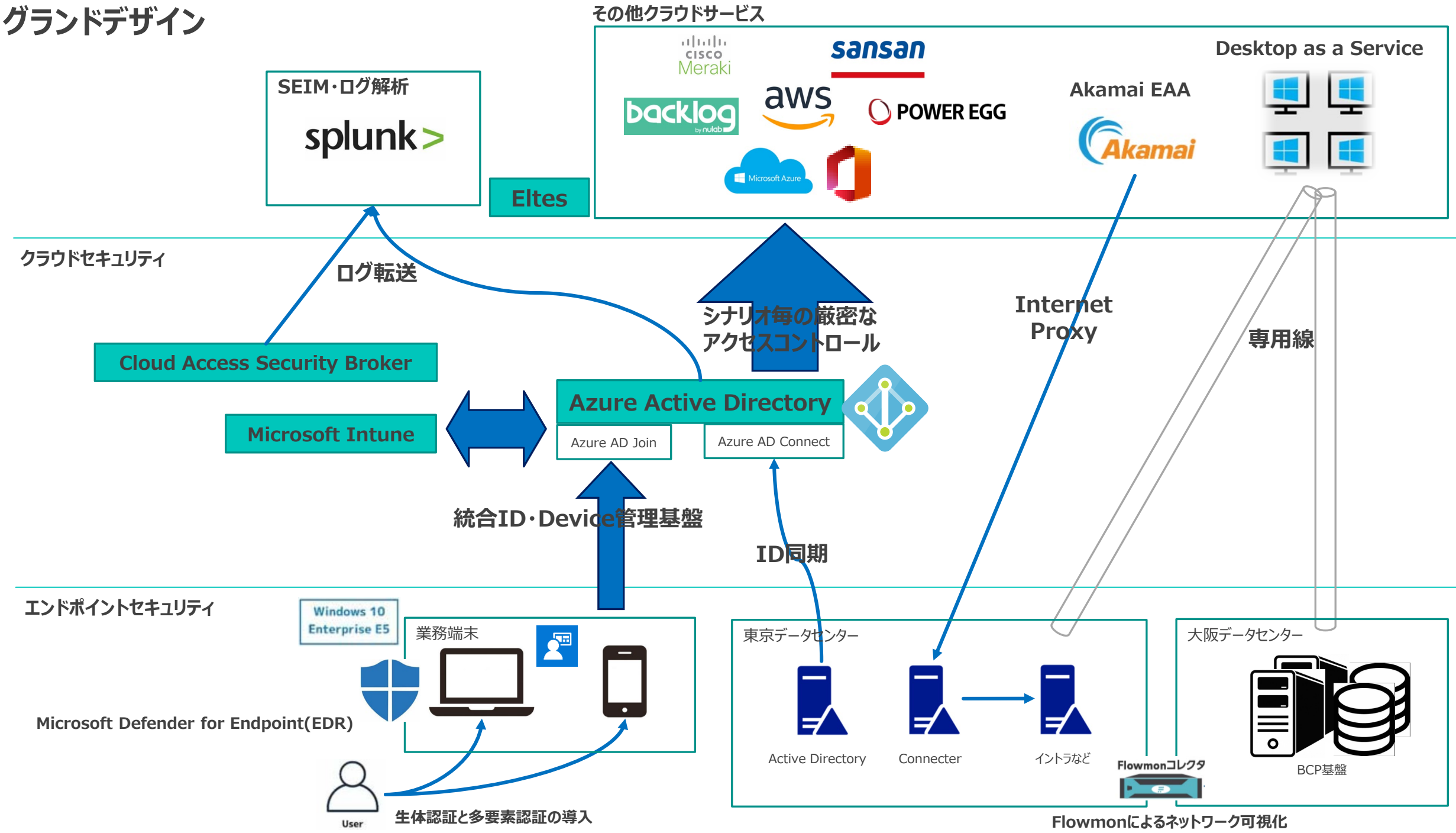
9つのAzure AD関連観点をふまえたゼロトラストの取り組みの概要

	Before	After（一部は既存環境併用継続/不要なものは漸減）
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
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，M365 E5 Exchange Online ATP(標的型攻撃保護)	WD Application Guard(コンテナベースのWeb分離環境)，WD ATP(EDR)，端末がWD 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,SSI等	Communication Compliance，Insider Risk Management，CASB/MCAS，DLP(データ損出防止)，自動暗号化/検出，Zscaler，PI等
09 監査	ログ定期分析，SIEM(Splunk ES)等	SIEM(既存 ＋ Azure Sentinel試行)，ゼロトラストベース等

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

WD：Windows Defender
その他各社の商標,略称等

グランドデザイン


その他クラウドサービス
cisco Meraki
sansan
backlog by nulab
aws
POWER EGG
Microsoft Azure
Desktop as a Service
Akamai EAA
Akamai
SEIM・ログ解析
splunk>
Eltes
クラウドセキュリティ
ログ転送
シナリオ毎の厳密な
アクセスコントロール
Internet
Proxy
専用線
Cloud Access Security Broker
Microsoft Intune
Azure Active Directory
Azure AD Join
Azure AD Connect
統合ID・Device管理基盤
ID同期
エンドポイントセキュリティ
Windows 10
Enterprise E5
業務端末
Microsoft Defender for Endpoint(EDR)
東京データセンター
Active Directory
Connecter
イントラなど
大阪データセンター
BCP基盤
Flowmonコレクタ
User
生体認証と多要素認証の導入
Flowmonによるネットワーク可視化

2 あの心配ごとと向かい合う

最近多いクラウドの事故・インシデントの話題

最近多いクラウドの事故・インシデントの話題

piyolog

クラウド の検索結果:

クラウド

2021-01-13

楽天モバイルへ転職したソフトバンク元社員の社外秘情報持ち出しについてまとめてみた

内部犯行 情報漏えい

...フトバンクの利用する クラウド サーバーに接続。営業秘密を含むファイルをフリーアドレス宛に添付、送信。*8 *9 ソフトバンクは退職後に返却された社有PCからメール送信の痕跡を確認し発覚。*10 ソフトバンクの追加施策 ソフトバンクは当該事案発生を受け、2020年3月以降次の追加施策による順次実施したと説明。 なお、これまで当社は、全社員に対して定期的に秘密保持契約の締結やセキュリティー研修などを実施してきましたが、今回の出来事を受けて、再発防止施策として以下の追加施策を2020...

119 users ★+ ★82★

2020-12-28

Salesforceの設定不備に起因した外部からのアクセス事案についてまとめてみた

意図せぬ公開 情報漏えい

...履歴について 楽天 クラウド 型営業管理システムへの社外の第三者によるアクセスについて イオン お問い合わせフォームへの社外の第三者によるアクセスについて イオン銀行 「来店予約・オンライン相談サービス」システムへの第三者による不正アクセスについて 国際観光振興機構 [PDF] クラウド 型情報管理システムへの第三者によるアクセスの可能性について バンダイ [PDF] クラウド 型営業管理システムの第三者による不正アクセスについて 東邦ガス ガスエネルギー館の クラウド 型システムへの...

286 users ★+ ★★★28★

2020-12-20

SolarWindsのサプライチェーン攻撃についてまとめてみた

APT 海外事例 サプライチェーン攻撃

...使い、オンプレミス、 クラウド 環境に対し不正なログインを行う。（この時使用されるSAMLトークンは独自の信頼できる証明書で署名されていることから検知を見落としている可能性を指摘。） この方法（あるいはそれ以外）で取得した特権アカウントを使い既存のアプリケーションプリンシパルに独自の資格情報を追加。 アプリケーションに割当たった権限でAPIの呼び出しを行う。 9．他に関連した出来事は？ (1) VOLEXITYの報告 www.volexity.com VOLEXITYは今回の事案に...

139 users ★+ ★24★

2020-08-12

7月下旬以降相次ぐ不審メール注意喚起についてまとめてみた

マルウェア感染

...お詫びとお知らせ （ クラウド ゲート） コンピュータウイルス感染に伴う「なりすましメール」発生に関するお詫びとお知らせ （マルツエレック） 不正メールの発生によるお詫びとお知らせ（亀屋良長） 当社社員を装う不審なメール（なりすましメール）に関するお詫びと注意喚起について（九電テクノシステムズ） 龍谷大学生活協同組合におけるPCウイルス感染と、感染に伴う不

プロフィール

piyokango (id:piyokango) PRO

読者になる 1561

@piyokangoさんをフォロー

検索

クラウド

最新記事

推進者として忘れてはいけないこと

びびらない

DXとは

Wikiの「段階」を参考に

1. デジタイゼーション　アナ→デジ
2. デジタライゼーション　ビジネスプロセス
3. DX

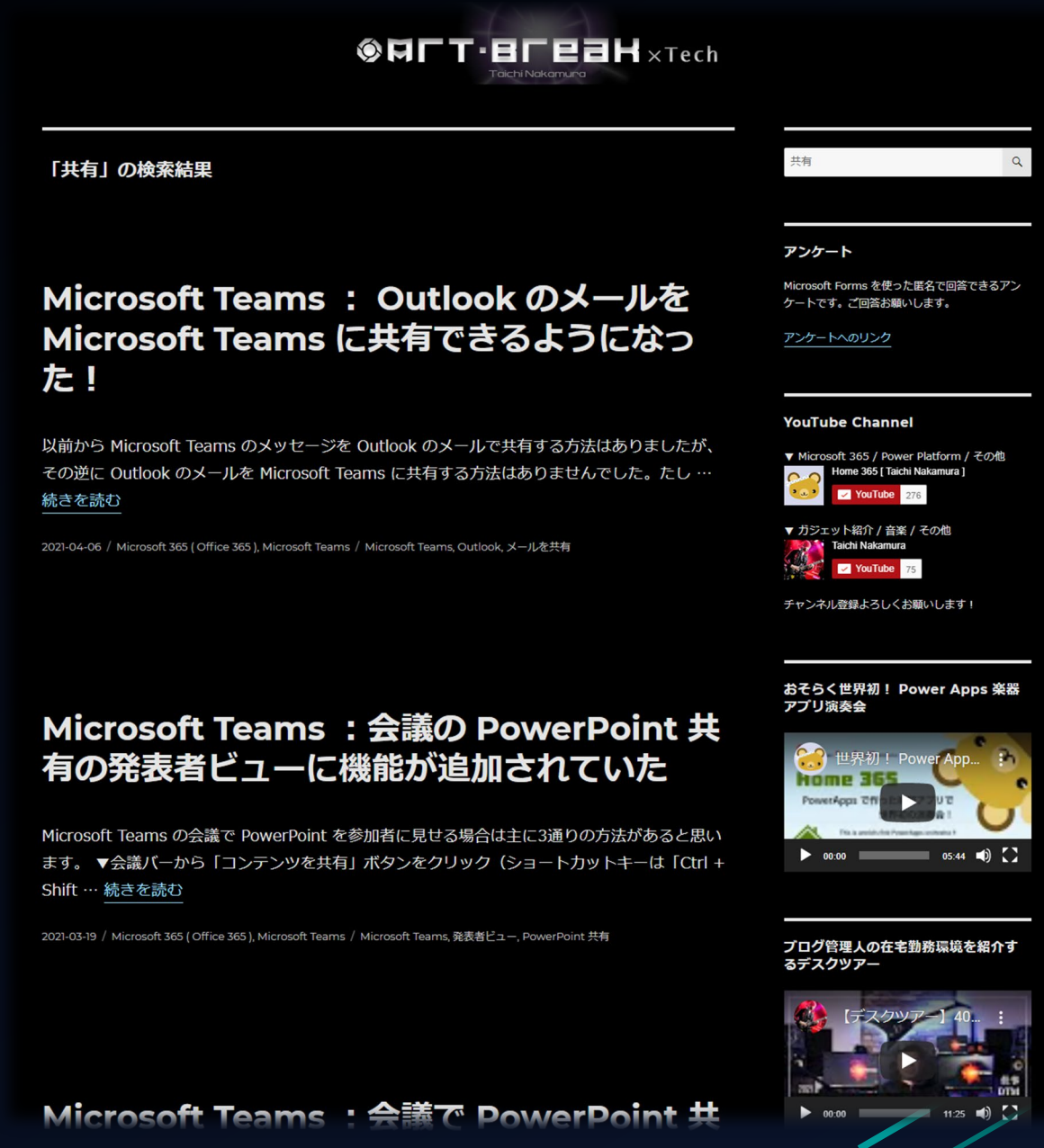
2以上　人、組織…が変わる

情報発信


Qiita
キーワードを入力
Qiitaユーザアンケートご協力のお願い/抽選でAmazonギフト券5000円プレゼント
LG TM
8
5
セキュリティ Advent Calendar 2020 25日目
@ishiayaya が2020年12月27日に更新 1414 views
Power BIのWeb公開と抑止
セキュリティ, PowerBI, PowerBIDesktop, MicrosoftLearn, PowerBIService
はじめに
Power BIでよいビジュアルができたので、組織内で共有を超えて、Webに公開～と。とても便利でよろしいのですが、組織としてPower BI Serivceを運用していたときに、知らない間で公開しちゃいけないレポートが公開されていた～ なんてことになっては困りますよね。なので、外部Web 公開の制御について、そして合わせて公開方法についても書きたいと思います。
免責等
「このように設定すべき」等はありませんし、主張するものではありません。各組織の運営に合わせたり、見直しの話し合い材料にしていただければと思います。また、組織の利用で一般資料者の方は、管理者権限がないために、管理者メニューが表示されないということもあります。ご了承を。
個人利用でのPower BI Service利用の場合は、自己の管理方法のご参考にどうぞ。
Web公開は外部への一般公開（Annoymous Access）のこと
通常、ビジュアルはオーサリングツールである、Power BI Desktop作り、発行（Pubish）で、Power BI Serviceに上げます。発行先を「マイワークスペース」にすると、自分だけのエリアへの発行になり、そこから組織内の人への共有でアクセス権を付与する等行うことができます。または、組織内にある他のワー

情報収集

Art-Break：Taichi Nakamura



さらなる手応えが欲しい

自分の設定やポリシーが正しいか
確かめたい

情報収集

オンラインセミナー

プロセス・コミュニケーション改革セミナー

ニューノーマル時代に向けた業務プロセス刷新とコミュニケーション促進の勘所

2020.12.22 火 13:30 -

プロセス・コミュニケーション改革セミナー　ニューノーマル時代に向けた業務プロセス刷新とコミュニケーション促進の勘所

Microsoft 365 情報漏洩対策のベスト プラクティス

AvePoint Japan
プロダクト マーケティング マネージャー／Microsoft MVP
中村 太一 氏

多くの組織で活用が進んでいる Microsoft 365。リモートワークを支える強力なツールとして活用が進む一方で、「情報漏洩をどう防止するか」 という課題に直面している IT 部門も少なくありません。本講演では、Microsot 365 で発生しがちな情報漏洩のシナリオと効果的な対策について、AvePoint の SaaS ツール・Policies & Insights（ポリシーズ・アンド・インサイツ）のご紹介も交えながらお話いたします。

3 なぜPIか

AvePoint

Microsoft 365 情報漏洩対策のベストプラクティス

Policies & Insights (PI)

2020年12月22日

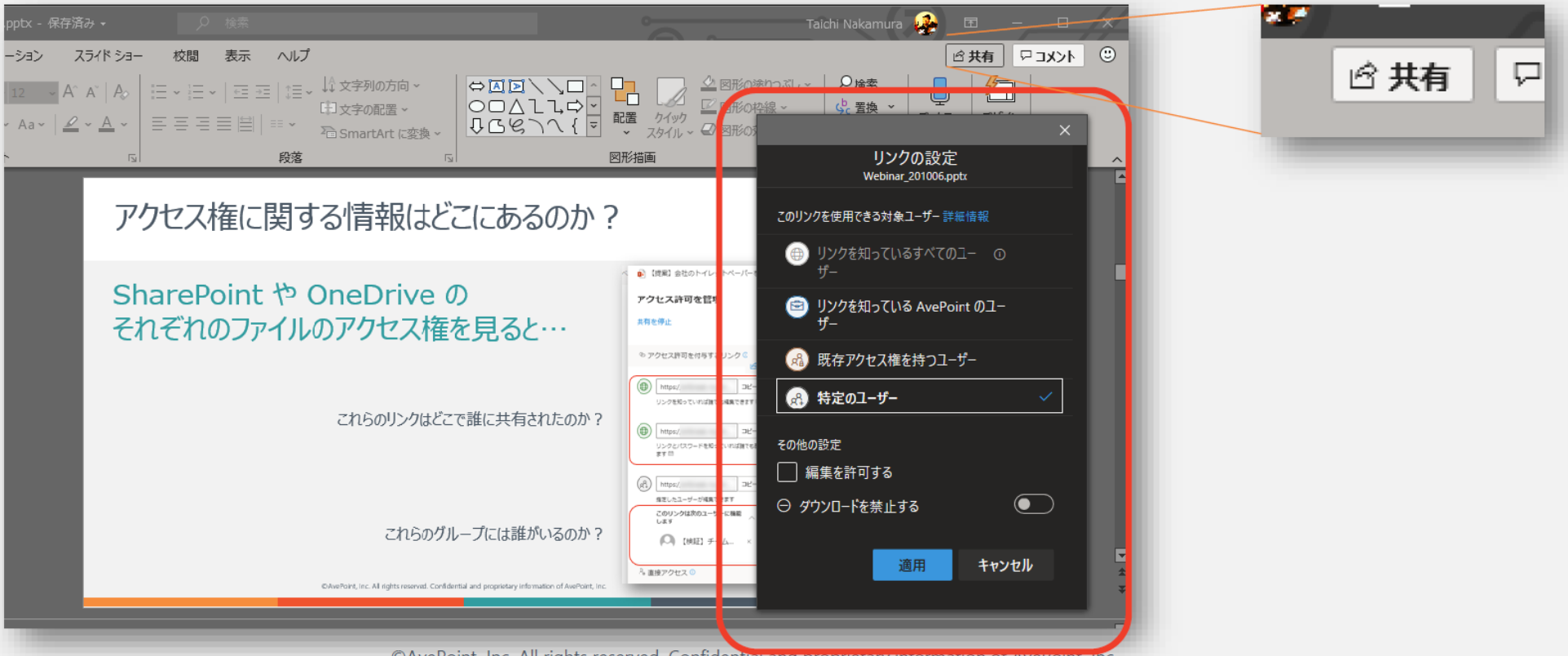
AvePoint Japan 株式会社
中村 太一 （ プロダクト マーケティング マネージャー ）

気になるのが、情報漏洩…

共有はカンタンだけど、アクセス権の確認は困難！

アクセス権の確認は困難・・・でも共有は簡単！？

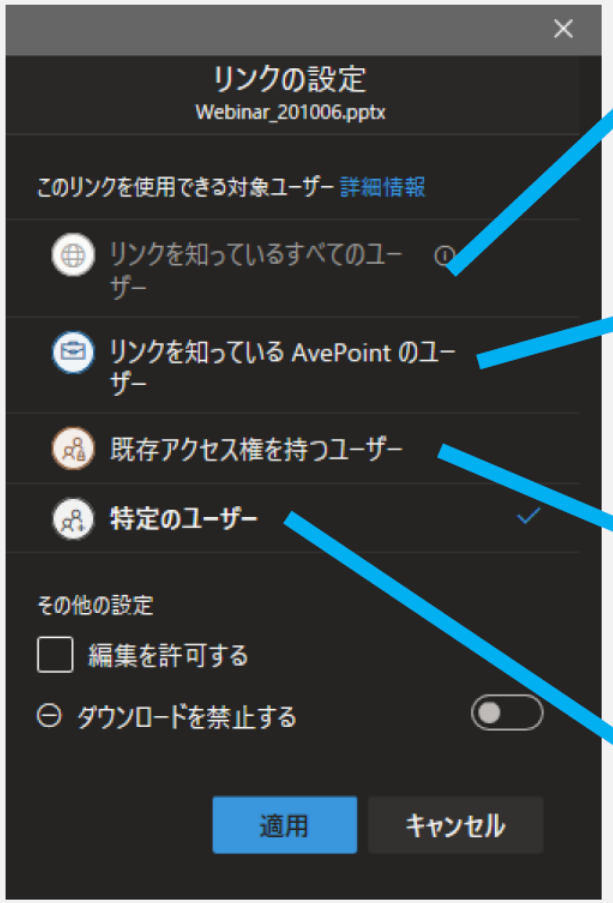
Office アプリの共有ボタンからドキュメントを簡単に共有できる



©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

おさらい：どうして**シャドウユーザー**が生まれるのか

※「シャドウユーザー」： SharePoint 内のファイルにはアクセスできるが、Microsoft Teams のチームメンバーではないユーザー



匿名リンク（外部も）

- 既定は無効化されている (ただし無効化されていない場合はハイリスク)

“外部以外は全員"

- 最もよく利用される共有方法 (一番わかりやすく簡単だから)

「既存のアクセス権」って、誰が持ってるの?

- 特に大きいグループが追加されている場合は、誰がアクセス権を持っているのか把握しづらい

「特定のユーザー」って、結局誰?

- ドキュメント単位で固有の権限が設定されるのが当たり前に！？

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

AvePoint

Policies & Insights

For Microsoft 365

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

AvePoint
Policies & Insights
For Microsoft 365

PI

パイ

Policies & Insights 概要

ご利用中のMicrosoft 365テナントへ
お客様の情報セキュリティポリシーに基いたシステムの正常性を継続的に維持管理します。

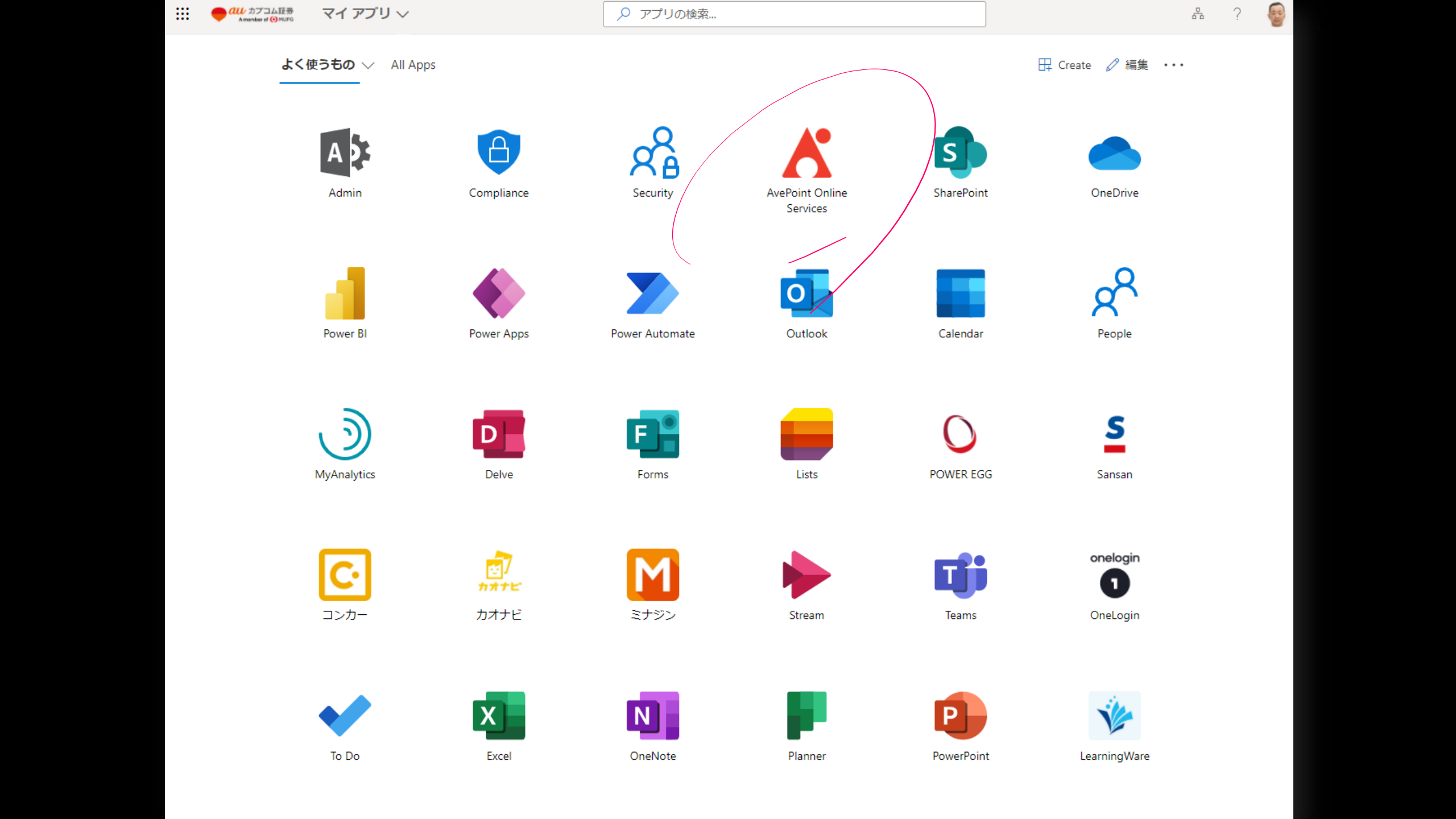
ポリシー定義 ＋ **実行/自動修正**

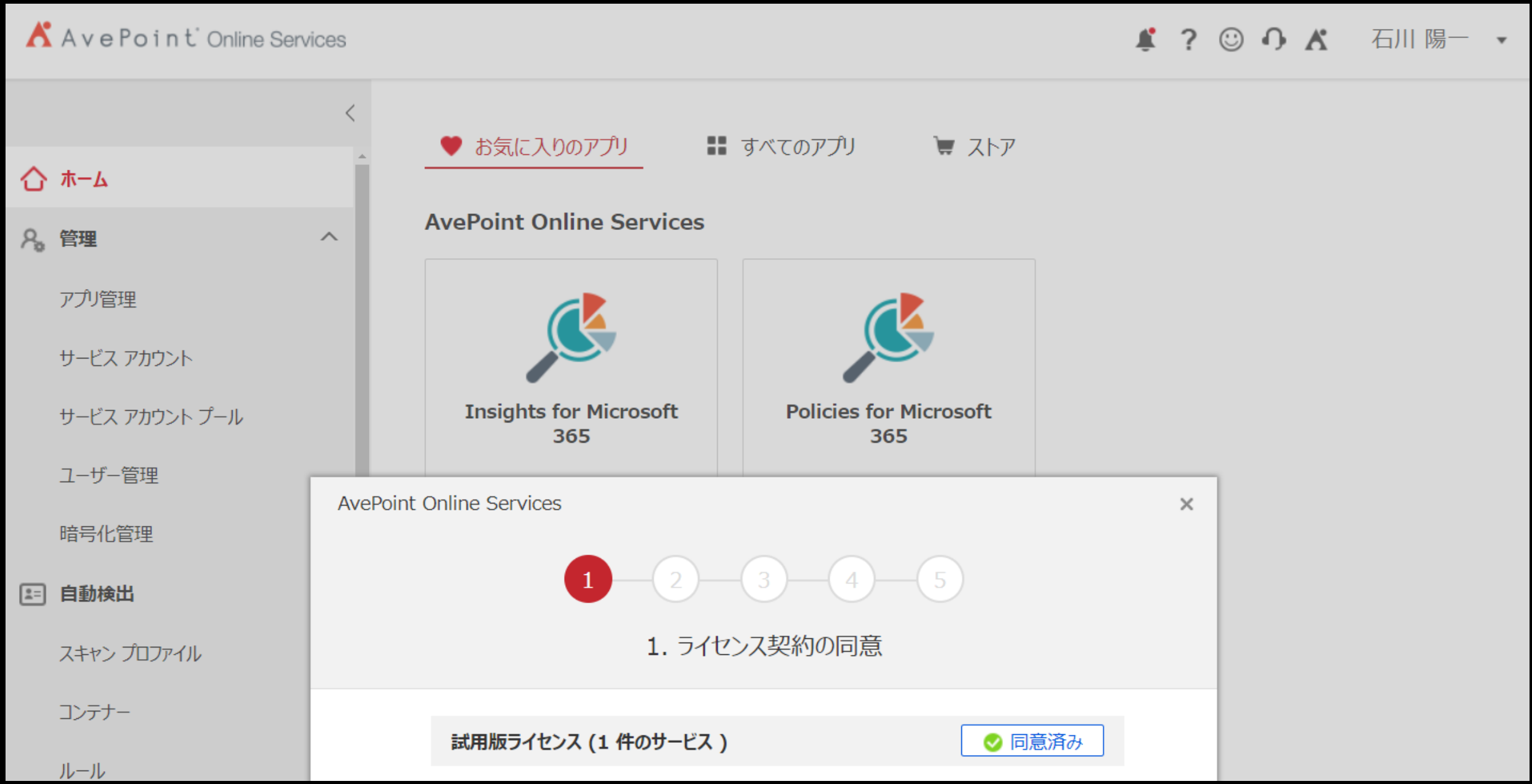
1. 定義ルールを利用したポリシーの定義
2. ポリシーの実行範囲の設定

1. アクセス権/コンテンツをポリシー違反時、自動的に是正実施
2. 膨大なポリシー違反時は、ITリソースを自動的に拡張し高速処理を実現

リスクの可視化

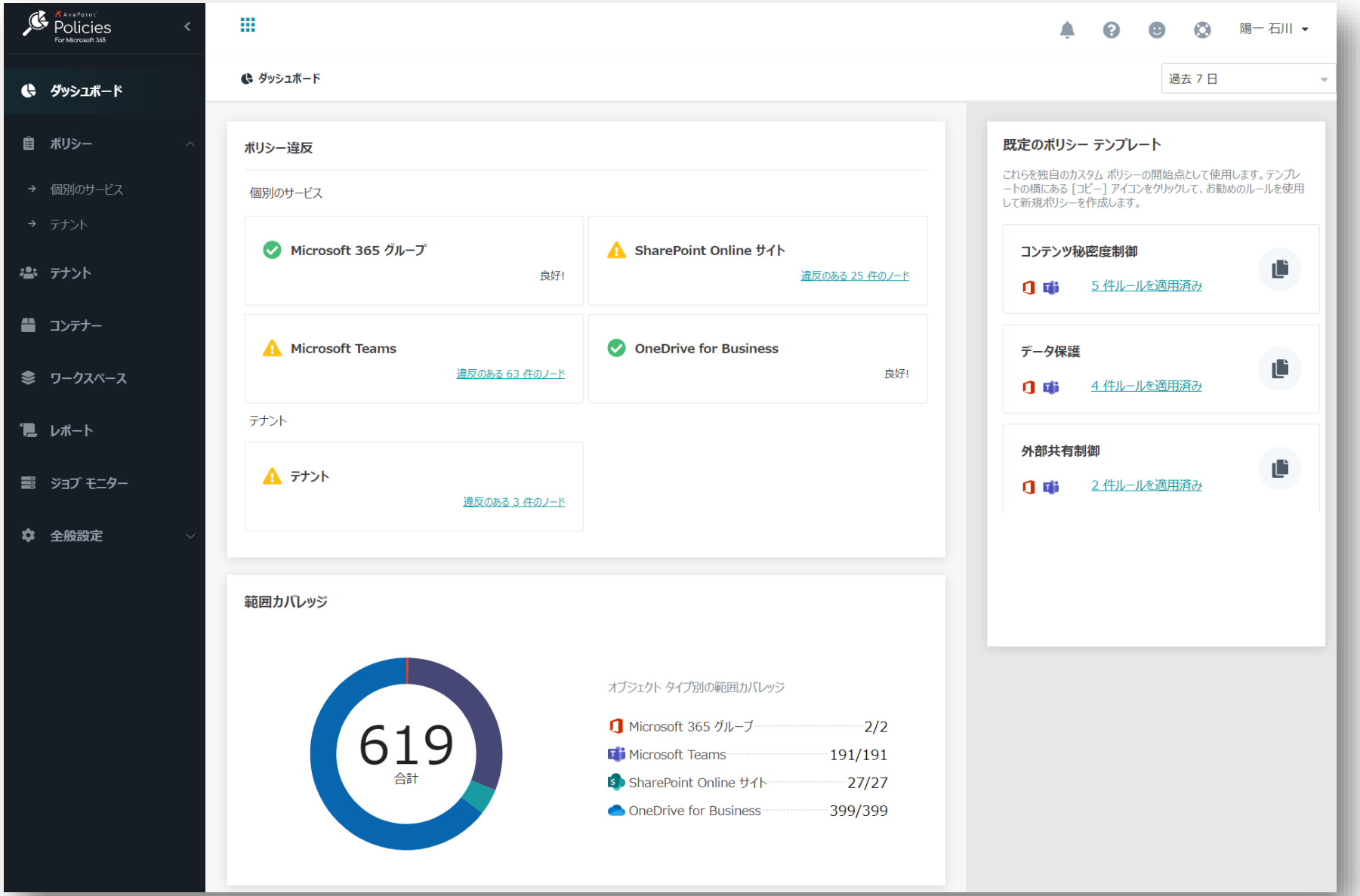
1. 機密情報（個人情報、クレジットカード情報等）に準ずるコンテンツの集計
2. 機密情報の格納場所/権限の調査
3. 特定ユーザのアクセス可能範囲の調査


マイ アプリ
アプリの検索...
よく使うもの
All Apps
Create
編集
Admin
Compliance
Security
AvePoint Online Services
SharePoint
OneDrive
Power BI
Power Apps
Power Automate
Outlook
Calendar
People
MyAnalytics
Delve
Forms
Lists
POWER EGG
Sansan
コンカー
カオナビ
ミナジン
Stream
Teams
OneLogin
To Do
Excel
OneNote
Planner
PowerPoint
LearningWare


AvePoint Online Services
石川 陽一
ホーム
管理
アプリ管理
サービス アカウント
サービス アカウント プール
ユーザー管理
暗号化管理
自動検出
スキャン プロファイル
コンテナー
ルール
お気に入りのアプリ
すべてのアプリ
ストア
AvePoint Online Services
Insights for Microsoft 365
Policies for Microsoft 365
AvePoint Online Services
1
2
3
4
5
1. ライセンス契約の同意
試用版ライセンス (1 件のサービス)
同意済み

AvePoint Policies For Microsoft 365

ポリシー定義 ＋ 実行/自動修正



AvePoint Policies For Microsoft 365

ポリシー定義 + 実行/自動修正

M365グループ関連

2021/02/08 石川 陽一

ルール

分類の強制

グループまたはチームの分類の変更を禁止します。

シャドウ ユーザーの削除

SharePoint Online サイトに対してアクセス権を持っているが、グループ / チーム メンバーシップに含まれていないユーザーを削除します。

AvePoint Policies For Microsoft 365

ポリシー定義 ＋ 実行/自動修正

ユースケース 3

利用シーン

ゲストユーザで一定期間アクセスがないユーザに対して、Azure AD のアカウントを削除する

ログ収集

ポリシー違反時、アカウント削除

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

AvePoint Policies For Microsoft 365

ポリシー定義 ＋ 実行/自動修正

ポリシー一覧（1）

監査モード　Microsoft 365のポリシーは、Microsoft 365の監査イベントを収集して、ポリシー外の設定を識別します。
スキャンモード　Microsoft 365のポリシーは、Microsoft 365の条件をスキャンして、ポリシー外の設定を識別します。

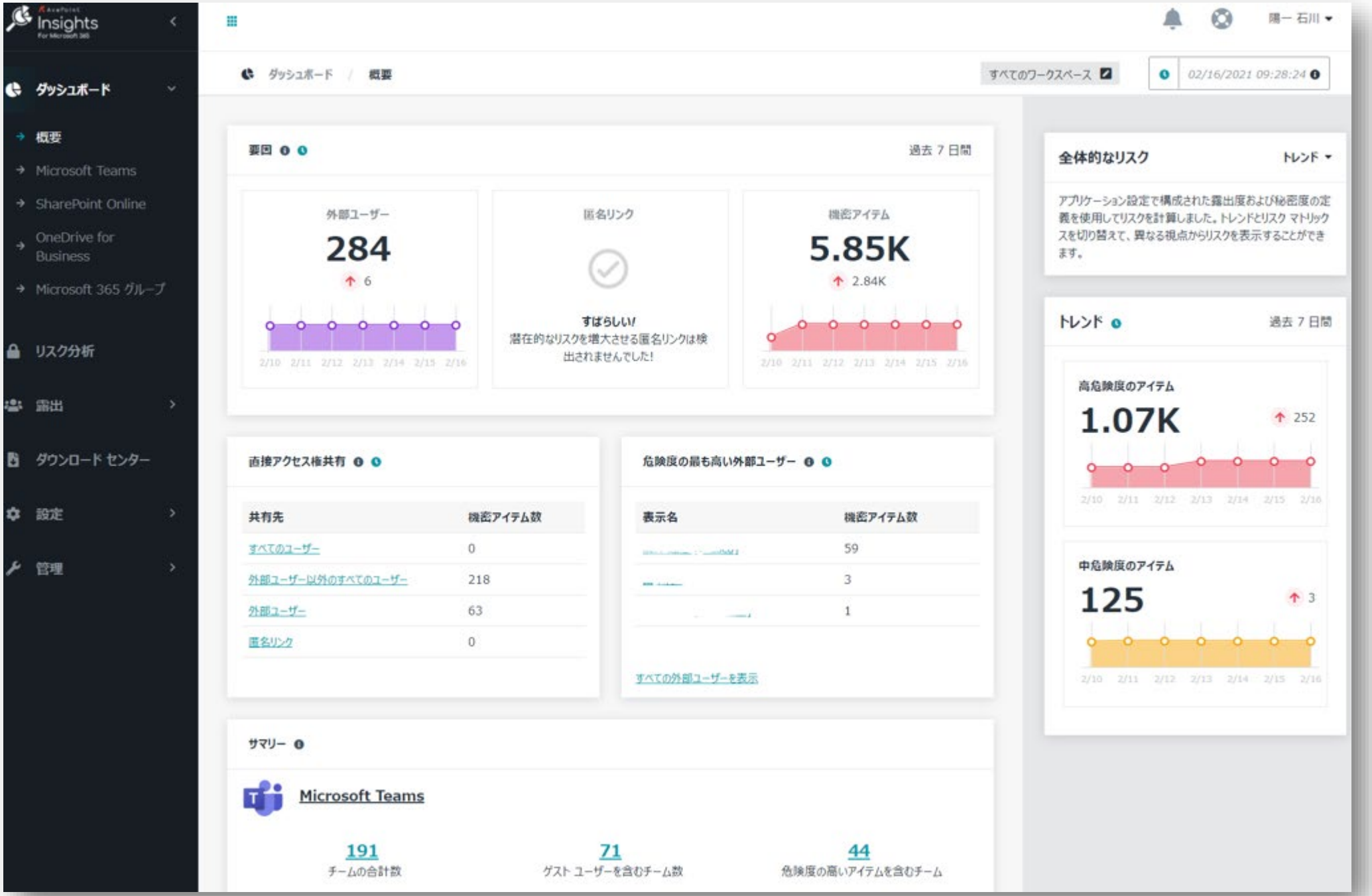
Microsoft 365 オブジェクトタイプで適用可能な個別ポリシー

	ルール	説明	データ検索モード	Microsoft 365 オブジェクトタイプ			
				SharePoint Onlineサイト	OneDrive for Business	Microsoft 365グループ (グループチームサイトを含む)	Microsoft Teams (グループチームサイトを含む)
1	アクセス要求設定	サイト内のアクセスリクエスト設定を制御して、サイトへのアクセスをリクエストおよび承認できるユーザーを管理します。	スキャンモード	●	●	●	●
2	分類の実施	グループまたはチームの分類の変更を防止します。	監査モード			●	●
3	コンテンツの作成とアップロードの制限	ユーザー、サイズ、ファイルタイプ、コンテンツタイプに基づいて、アイテム、添付ファイル、ドキュメントを含むコンテンツの作成とアップロードを制御します。	監査モード	●	●	●	●
4	削除制限	サイト内のオブジェクトを削除する機能を持つユーザーとグループを制御します。	監査モード	●	●	●	●
5	直接共有の禁止	ユーザーが個人とコンテンツを直接共有できないようにします。	監査モード	●	●		
6	外部共有設定	グループまたはチームの外部共有設定を制御します。	スキャンモード			●	●
7	グループ / チーム作成の制限	グループまたはチームを作成する機能を持つユーザーを制御します。	監査モード			●	●
8	リスト/ライブラリオブジェクト数の制限	リスト/ライブラリ内のアイテム、ドキュメント、およびフォルダーの数を制御します。	スキャンモード	●	●	●	●
9	メンバーシップの制限	グループまたはチームにメンバーとして追加できるユーザーを制御します。	スキャンモード			●	●
10	チーム名の強制	チームの所有者が作成後にチームの名前を変更できないようにします。	監査モード				●
11	Outlookクライアントでの Microsoft 365グループの可視性	Microsoft 365グループがOutlookクライアントに表示されるかどうかを制御します。	スキャンモード			●	●

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

AvePoint Insights For Microsoft 365

リスクの可視化



EX_TF_AvePoint

EX_TF_AvePoint

チーム

メンバー　保留中の要求　チャネル　設定　分析　アプリ

すべてのチャネル　過去 90 日間　2021/01/15 - 2021/04/14

要約

10	8	0	51.43 MB
ユーザー	アプリ	会議	SharePoint ファイル

エンゲージメント

8	168	131	68
投稿	返信	メンション	リアクション

アクティブ ユーザー

10
アクティブ ユーザー

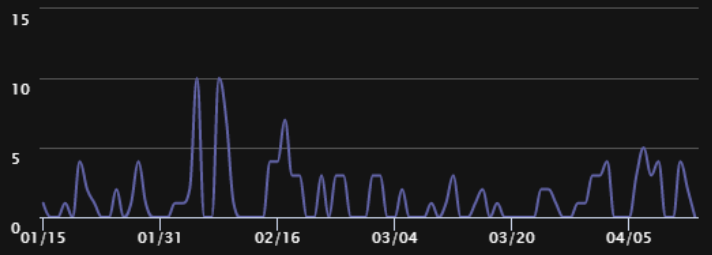
0
アクティブでないユーザー

役割

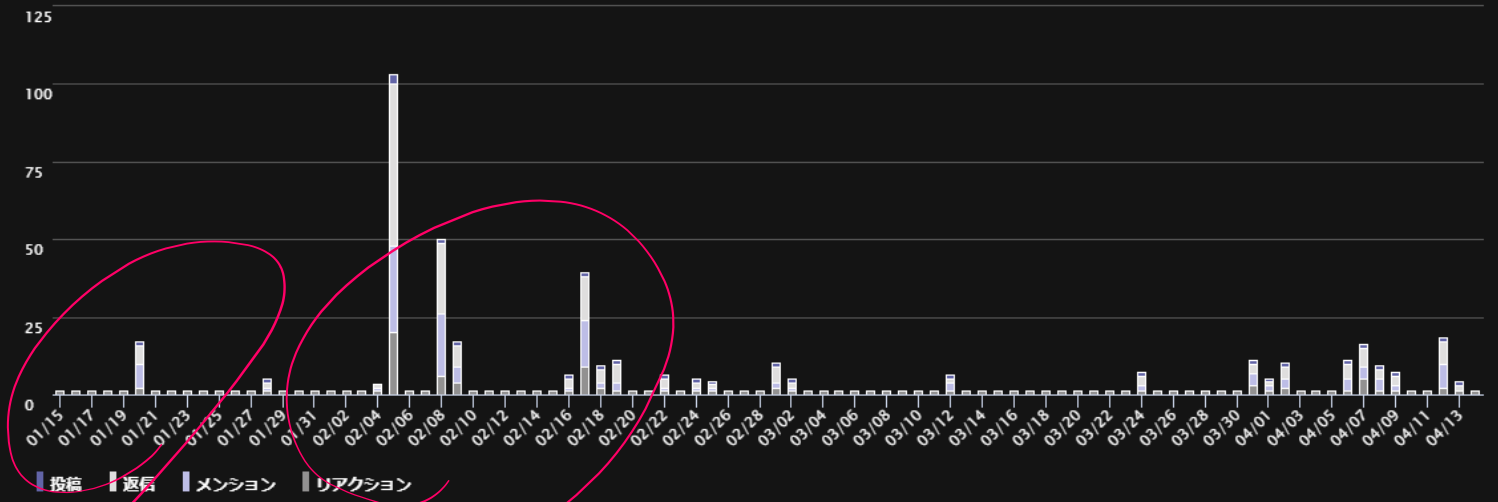
3
所有者とメンバー

7
ゲスト

アクティブ ユーザー



エンゲージメント



まとめ

まとめ

1. 弱さの認識は見直しの機会になる
2. 現場から変えていこうと動いてきた
3. 365でローコードや可視化は身近に
4. 人、組織のトランスフォームを受け入れる
5. ゼロトラストでは安全の可視化、大事

thank you

Gracias	ευχαριστώ	Danke	Grazie	благодаря
Hvala	Obrigado	Kiitos	شكراً	Tak
Ahsante	Teşekkürler	متشكرم	Salamat Po	감사합니다
Cám ơn	شكريه	Terima Kasih	Dank u Wel	Děkuji
நன்றி	Köszönöm	ありがとうございます	ขอบคุณครับ	Dziękuję
谢谢	Tack	Mulţumesc	спасибо	Merci
תודה	多謝晒	дякую	Ďakujem	धन्यवाद

#shifthappens