

ACTIONABLE STRATEGIES

IN THE MICROSOFT 365 WORLD

📅 April 20-22, 2021 📍 48 Hour Global Virtual Event

www.shifthappens.to/conference

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
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 になってみよう!」 #TryCivicEngr



略歴

富山出身。奥中(八村壘)、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



@ishiayaya



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



1 DXとゼロトラスト、 これまでの取り組み

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

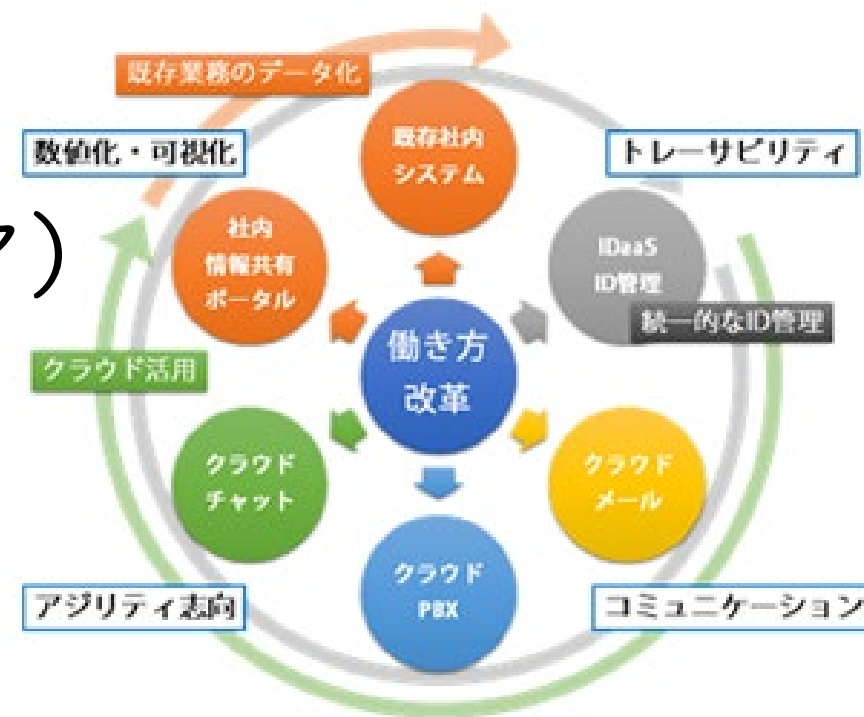
カブドットコム証券株式会社（代表執行役社長：齋藤 正勝、証券コード：8703、以下「当社」）は、「デジタルトランスフォーメーションを後押しする抜本的な働き方改革」をテーマとし、「クラウドとテレワークを活用したIT主導での生産性向上」を目指す社内業務改革の取り組みを開始しました。

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



onelogin



(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

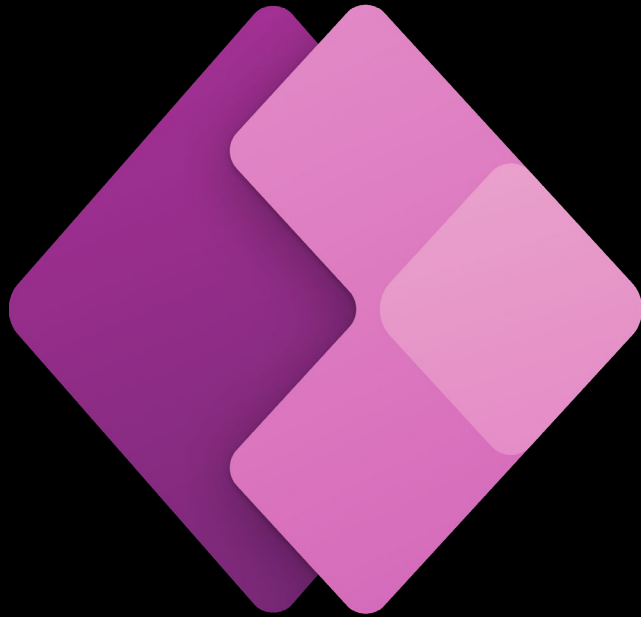
一般

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）	
				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
			従業員名														
			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	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
派遣社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														
正社員	システム	β	F														

予定をExcelに入力するんだ
200人共有でバーン!





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





テレワーク・時差出勤 登録状況 簡易版

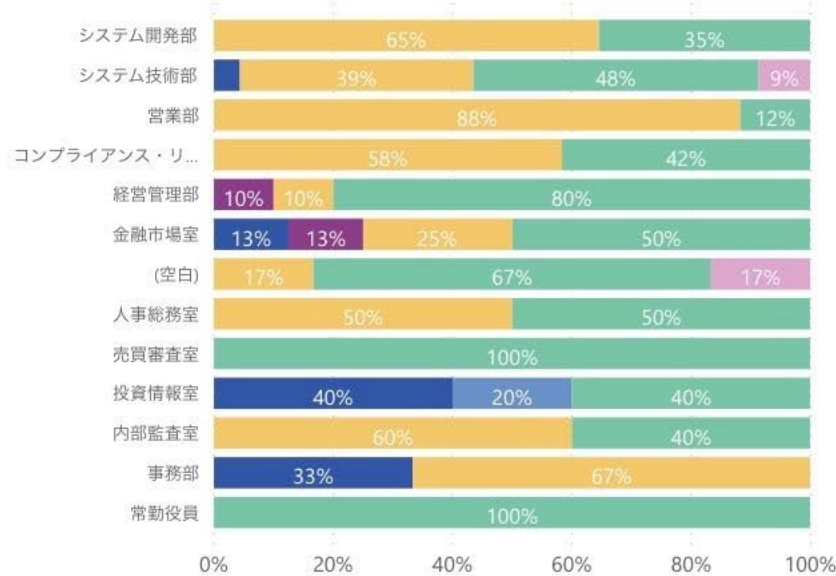
69

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

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



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



日 名前

- 3
- 3
- 3
- 3
- 3

Gr	場所等	時差出勤
マブチ管理グループ	テレワーク	09:00-18:00
フロント2グループ	テレワーク	08:30-17:30
	テレワーク	08:30-17:30
企画グループ	出社	08:00-17:00
システムリワーク管理グループ	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

35

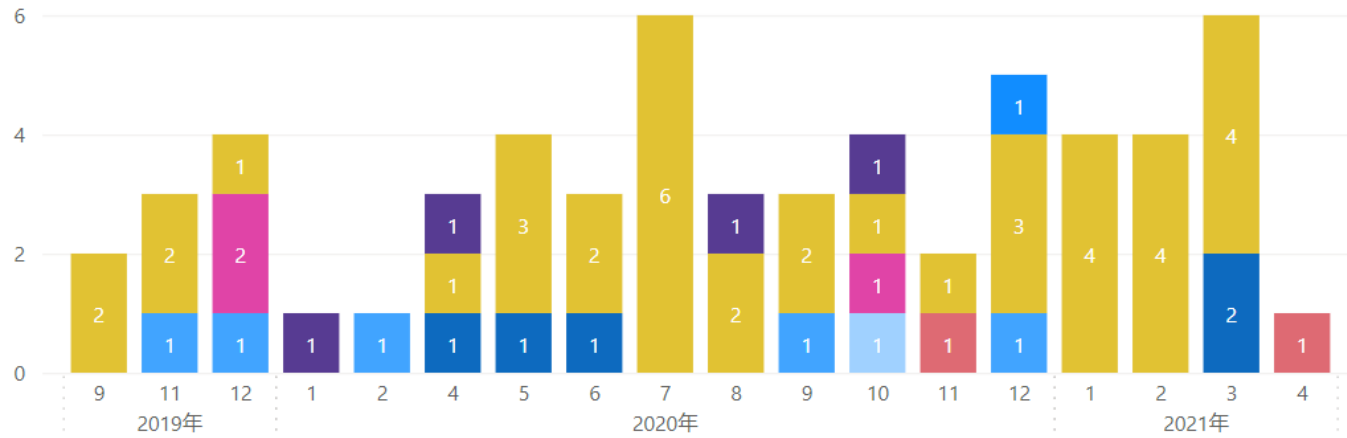
2020年の登壇回数

15

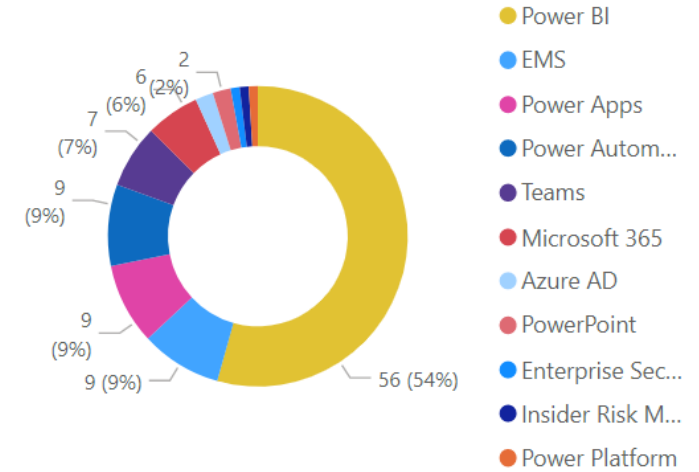
2021年の登壇回数

月毎の推移

主な分野 ● Azure AD ● EMS ● Microsoft 365 ● Power Apps ● Power Automate ● Power BI ● PowerPoint ● Teams



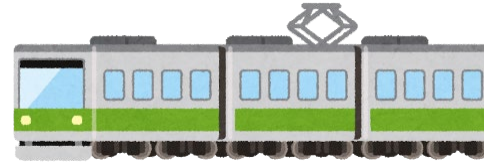
関連分野



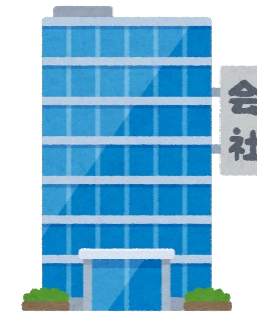
Date	活動	主な貢献分野	その他の貢献分野
2021/04/22	AvePoint #ShiftHappens 登壇 セキュリティ関連	Microsoft 365	EMS
2021/03/28	Power Automate Desktop勉強会 vol.2 LT 「Power Automate DesktopでPDF関係やってみた」	Power Automate	Power BI
2021/03/28	市民開発者 なってみよう! #5 自コミュニティ 「軽いPower Automate」	Power Automate	Power BI
2021/03/27	日本を元気に・革新コンソーシアム [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



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

貸与iPhoneの場合の主な考慮事項



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 テナント構成
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,
M365 E5 Exchange Online ATP(標的型攻撃保護)

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,SSI等

09 監査
ログ定期分析, SIEM(Splunk ES)等

After (一部は既存環境併用継続/不要なものは漸減)

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, Win 10 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

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

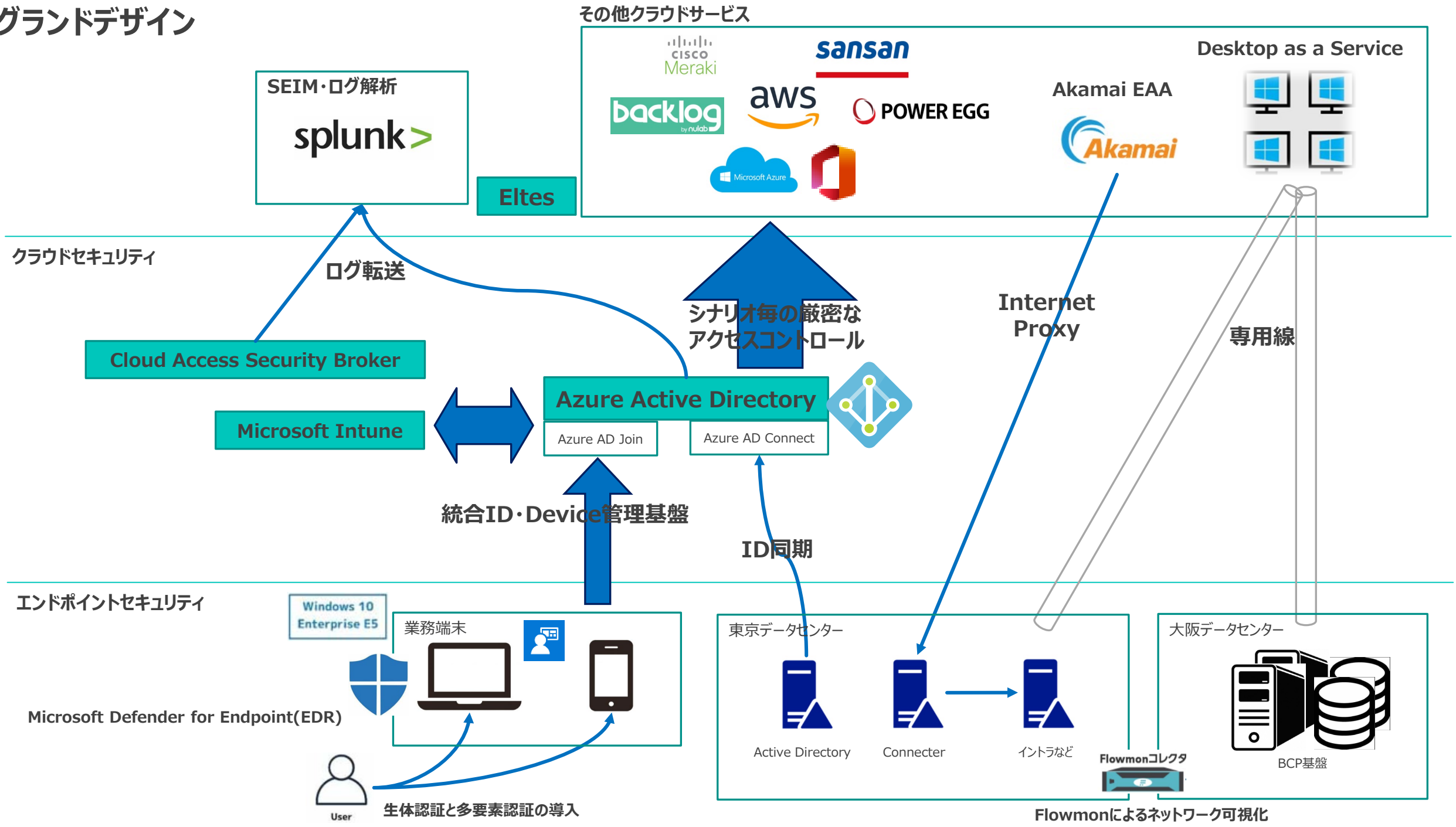
Azure AD B2B, 外部も2要素化, Teamsゲストユーザー運用確立


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

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/MCAS, DLP(データ損出防止), 自動暗号化/検出,
Zscaler, PI等

SIEM(既存 + Azure Sentinel試行), ゼロトラストベース等

グラウンドデザイン





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

クラウド セキュリティ 事故



🔍 すべて 📰 ニュース 🖼️ 画像 🛍️ ショッピング 🎬 動画 ⋮ もっと見る ⚙️ 設定 🛠️ ツール

約 4,190,000 件 (0.31 秒)

<https://www.acrovision.jp> > tech ▾

クラウドセキュリティ～過去事例と現在～ ITエンジニア向け ...

2020/07/13 — クラウドは数クリックで始められるので、手軽でとても便利です。ただ、だからと言って何の知識も持たずに始めるのは危険でしょう。本記事では過去に起きたクラウドのセキュリティに関する事故事例と、クラウドの ...

<https://www.cloudsecurityalliance.jp> > 2018/12 > t... ▾ PDF

クラウドの重大セキュリティ脅威 +

そういった基準が整わない状態では、ビジネスはセキュリティ事故に対して脆弱となり、クラウドへのシフトで得られる利点を失うことにもなりかねない。Cloud Security Alliance (CSA) は、クラウドコンピューティングの利点とリスクの ...

<https://www.nri-secure.co.jp> > blog > key-points-to-pre... ▾

クラウドからの情報漏洩、原因となる「設定ミス」を防止する ...

2020/02/28 — 昨今、クラウドサービスの利用が一般的になる一方で、設定ミスによる意図せぬ情報漏えいや不正アクセスが発生 ... 企業を取り巻く環境が大きく変化しているなか、クラウド特有のリスクを見逃した結果、セキュリティ事故に ...

<https://www.soumu.go.jp> > security > business > case ▾

事例13：クラウドサービスに預けていた重要データが消えた ...

総務省 安心してインターネットを使うために 国民のための情報セキュリティサイト ... クラウドサービスを利用していても、事業者側の障害やメンテナンスなどで利用できなくなることを想定して、バックアップを取得したり、サービス停止時 ...

<https://www.fujitsu.com> > security > secure > column ▾

クラウドサービス上の情報漏洩事故の防止の有効打として期待 ...

クラウドサービスにおけるセキュリティテクノロジーでは、新たな手法として「CASB (Cloud Access Security Broker : キャスビー)」が注目されています。提唱者によれば、CASBには大きく4つの機能があるとのこと。 「CASB」の4 ...

<https://cybersecurity-jp.com> > security-incident-case ▾

セキュリティインシデント事例 - サイバーセキュリティ

2019年8月23日、クラウドサービスのAWSで大規模な障害が発生しました。これにより、多くのサービスが停止し... 2019.08.28. コンプライアンスは法令を含む社会 ...

<https://japan.zdnet.com> > セキュリティ ▾

2020年の10大セキュリティ事件、トップは「ドコモ口座 ...

2020/12/17 — 一方で、クラウドセキュリティの実施状況やクラウド上のデータ侵害の経験についての回答からは、実際に顧客企業から聞いている内容と乖離（かいり）する部分や不自然な結果（情報漏えいの原因のトップに暗号化を主と ...

<https://securesamba.com> > media ▾

クラウドセキュリティの事故事例を最新の安全対策と合わせて ...

2019/02/21 — クラウドセキュリティの事故事例やその原因、対策について解説しています。リスク管理を正しく行うことで事故の危険性を減らすことができます。日々進化するネットの脅威への対策を徹底しましょう。

page: 2

<https://www.ibm.com> > downloads > cas ▾ PDF

2020年のサイバーセキュリティ：脅威と対策の総点検 - IBM

経営に大きな影響を及ぼすセキュリティ事件・事故が増加。2018年 A社製造業・顧客情報をクラウド上で公開・クラウドストレージの設定ミス、顧客情報の流出、2019年 B社流通業・アカウントの不正利用・ガイドライン未遵守のままシステムが ...

<https://www.ibm.com> > cas > GJMDPMV9 ▾ PDF

マルチクラウド時代の最大の懸念「セキュリティ」確保 ... - IBM

これに対しクラウドでは便利。になった反面、設定ミスが直接、セキュリティ事故に、つながってしまう」（赤松氏）。こうした事態に自ら気、付けず、第三者の指摘によってはじめて判明した場合、は、企業に与える損失や影響 ...

<https://news.mynavi.jp> > TECH+ > 企業IT > セキュリティ ▾

ラック、AWSでの事故原因・対応などまとめたクラウド ...

2020/01/31 — ラックは1月30日、同社のサイバー救急センターが事故調査で得た情報を基にサイバー攻撃の動向などを分析した「サイバー救急センター ... ラック、AWSでの事故原因・対応などまとめたクラウドセキュリティレポート。

<https://news.mynavi.jp> > itsearch > article > security ▾

クラウドサービス利用で複雑化する事故対応 - 第6回「情報 ...

2021/03/30 — 不幸にもセキュリティ事故に遇ってしまったものの、その後の対応が素晴らしかった企業を表彰する「情報セキュリティ事故対応アワード」審査員。第6回目となる今回は、2021年2月26日にオンライン開催された。

<https://enterprise.verizon.com> > ja-jp > learn-the-basics ▾

クラウドのセキュリティリスクトップ10とその対処方法

現在上位にランクインしているクラウドのセキュリティリスクについて、Verizon Enterprise Solutionsが最新の情報をお届けいたします。 ... クラウドサービスプロバイダーが誤ってデータを削除してしまう事故が起こる可能性もあるのです。

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てられた権限で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 (丸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



+ 読者になる 1561

@piyokangoさんをフォロー

検索

クラウド

最新記事

改ざんされた官房長官記者会見画像のTwitter投稿についてまとめてみた [251 users](#)

データ入力不備で全国展開が先送りされたマイナンバーカードの保険証利用についてまとめてみた [71 users](#)

業務委託先元従業員による松井証券の不正送金事案についてまとめてみた [197 users](#)

管理不備と報じられたLINEの問題についてまとめてみた [780 users](#)

攻撃発生中のExchange Serverの脆弱性 ProxyLogonなどについてまとめてみた [78 users](#)

データ移行で発生したみずほ銀行のシステム障害についてまとめてみた [706 users](#)

米国で発生した浄水システムの不正操作についてまとめてみた [96 users](#)

最恐ウイルスEmotetをテイクダウンしたOperation Ladybirdについてまとめてみた [295 users](#)

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 [119 users](#)

福岡県の新型コロナ陽性者情報流出についてまとめてみた [184 users](#)

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
3. DX ビジネスプロセス

2以上

人、組織…が**変**わる





8



5



セキュリティ Advent Calendar 2020 | 25日目

@ishiyaya 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。とても便利でよいのですが、組織としてPower BI Service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て、見直しの話し合い材料に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（Anonymous 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（Publish）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



「共有」の検索結果

Microsoft Teams : Outlook のメールを Microsoft Teams に共有できるようになった!

以前から Microsoft Teams のメッセージを Outlook のメールで共有する方法はありましたが、その逆に Outlook のメールを Microsoft Teams に共有する方法はありませんでした。たし ... [続きを読む](#)

2021-04-06 / Microsoft 365 (Office 365), Microsoft Teams / Microsoft Teams, Outlook, メールを共有

Microsoft Teams : 会議の PowerPoint 共有の発表者ビューに機能が追加されていた

Microsoft Teams の会議で PowerPoint を参加者に見せる場合は主に3通りの方法があると思います。▼会議バーから「コンテンツを共有」ボタンをクリック (ショートカットキーは「Ctrl + Shift ... [続きを読む](#)

2021-03-19 / Microsoft 365 (Office 365), Microsoft Teams / Microsoft Teams, 発表者ビュー, PowerPoint 共有

Microsoft Teams : 会議で PowerPoint 共

共有

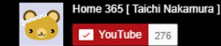
アンケート

Microsoft Forms を使った匿名で回答できるアンケートです。ご回答お願いします。

[アンケートへのリンク](#)

YouTube Channel

▼ Microsoft 365 / Power Platform / その他



▼ ガジェット紹介 / 音楽 / その他



チャンネル登録よろしくお願います!

おそらく世界初! Power Apps 楽器アプリ演奏会



ブログ管理人の在宅勤務環境を紹介するデスクツアー



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

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、Microsoft 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（ポリシース・アンド・インサイト）のご紹介も交えながらお話いたします。



3 なぜPIか



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）

Unleash the Power of You

Accessible content is available upon request.

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

リンクの設定
Webinar_201006.pptx

このリンクを使用できる対象ユーザー 詳細情報

- リンクを知っているすべてのユーザー
- リンクを知っている AvePoint のユーザー
- 既存アクセス権を持つユーザー
- 特定のユーザー

その他の設定

- 編集を許可する
- ダウンロードを禁止する

適用 キャンセル



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！？





 AvePoint

Policies & Insights

For Microsoft 365





AvePoint

Policies & Insights

For Microsoft 365

PI

パイ



検知と
優先順位決定



モニタリングと
修正



環境を安全な
まま維持

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づ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

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

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. 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

- ダッシュボード
- ポリシー
 - 個別のサービス
 - テナント
- テナント
- コンテナ
- ワークスペース
- レポート
- ジョブ モニター
- 全般設定



ダッシュボード

過去 7 日

ポリシー違反

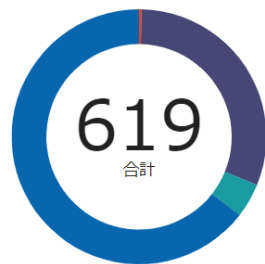
個別のサービス

Microsoft 365 グループ 良好!	SharePoint Online サイト 違反のある 25 件のノード
Microsoft Teams 違反のある 63 件のノード	OneDrive for Business 良好!

テナント

テナント 違反のある 3 件のノード

範囲カバレッジ



オブジェクト タイプ別の範囲カバレッジ

Microsoft 365 グループ	2/2
Microsoft Teams	191/191
SharePoint Online サイト	27/27
OneDrive for Business	399/399

既定のポリシー テンプレート

これらを独自のカスタム ポリシーの開始点として使用します。テンプレートの横にある [コピー] アイコンをクリックして、お好みのルールを使用して新規ポリシーを作成します。

コンテンツ秘密密度制御

[5 件ルールを適用済み](#)

データ保護

[4 件ルールを適用済み](#)

外部共有制御

[2 件ルールを適用済み](#)



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。

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





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			●	●



- ダッシュボード
- 概要
- Microsoft Teams
- SharePoint Online
- OneDrive for Business
- Microsoft 365 グループ
- リスク分析
- 露出
- ダウンロードセンター
- 設定
- 管理

ダッシュボード / 概要 すべてのワークスペース 02/16/2021 09:28:24

要約

過去 7 日間

外部ユーザー

284

↑ 6

匿名リンク

✓

すばらしい!
潜在的なリスクを増大させる匿名リンクは検出されませんでした!

機密アイテム

5.85K

↑ 2.84K

直接アクセス権共有

共有先	機密アイテム数
すべてのユーザー	0
外部ユーザー以外のすべてのユーザー	218
外部ユーザー	63
匿名リンク	0

危険度の最も高い外部ユーザー

表示名	機密アイテム数
...	59
...	3
...	1

[すべての外部ユーザーを表示](#)

サマリー

Microsoft Teams

191 チームの合計数	71 ゲスト ユーザーを含むチーム数	44 危険度の高いアイテムを含むチーム
-----------------------	------------------------------	-------------------------------

全体的なリスク

トレンド

アプリケーション設定で構成された露出度および秘密度の定義を使用してリスクを計算しました。トレンドとリスクマトリックスを切り替えて、異なる視点からリスクを表示することができます。

トレンド

過去 7 日間

高危険度のアイテム

1.07K

↑ 252

中危険度のアイテム

125

↑ 3



メンバー 保留中の要求 チャンネル 設定 分析 アプリ

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

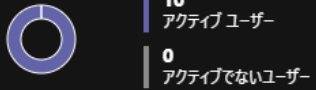
要約

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

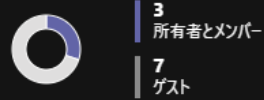
エンゲージメント

8 投稿 168 返信 131 メンション 68 リアクション

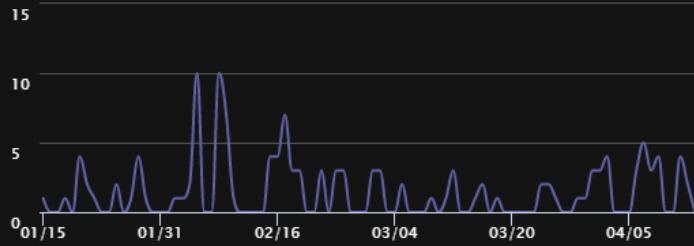
アクティブ ユーザー



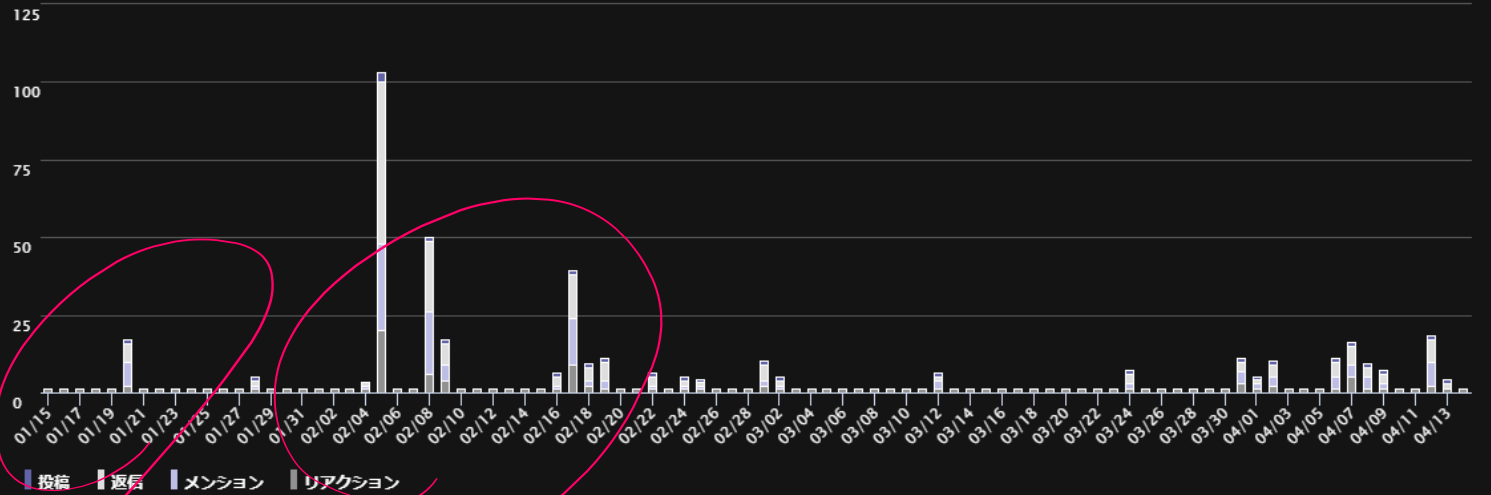
役割



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

متشكراً

Salamat Po

감사합니다

Cám ơn

شكريه

Terima Kasih

Dank u Wel

Děkuji

நன்றி

Köszönöm

ありがとう
ございます

ឧបត្ថម្ភ

Dziękuję

谢谢

Tack

Mulțumesc

спасибо

Merci

תודה

多謝晒

дядкую

Ďakujem

धन्यवाद