Skype for Businessにおける個人情報、機密情報の漏洩対策

Skype for Business コンプライアンス ガード

FairUSE

フェアユース株式会社

当資料の要約

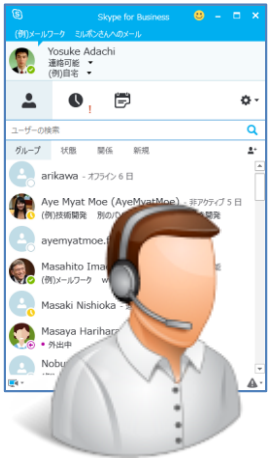
Skype for Business Server / Onlineでは管理者に対して提供されているアーカイブ、インプレースホールド＆訴訟ホールドではログを取得することが出来ない利用パターンが明確に存在しています。（当資料6、7ページ参照）

このため情報漏洩の発生確認後でさえも、証左としてのログが存在せず、情報漏洩ルートを提示出来ないことが御座います。

Skype for Businessコンプライアンスガードでは全ての利用パターンのログを記録し、また疑わしいIMテキスト、ファイル転送が発生した場合に、IT管理者にアラート送信します。

Skype for Business Server/Onlineの情報漏洩の危険性

Skype for Business Server / Onlineにはログ機能としてのアーカイブ、インプレースホールド/訴訟ホールドのログ機能はありますが、Skype for Businessの利用内容の全てのログの取得が可能ではありません。企業内での個人情報、機密情報の漏洩の危険性があります。



社内でも本来は機密情報を閲覧できない立場のユーザ

社内

コンプライアンス違反

- 明日発表予定の決算報告書
- 申請前の特許情報
- 特定の個人の契約情報

社内

社内で機密情報を取り扱う立場のユーザ

全てのログが残るわけではなく、情報漏洩が発生しても追跡できないため問題の対応が出来ない。また監査に耐えられない。

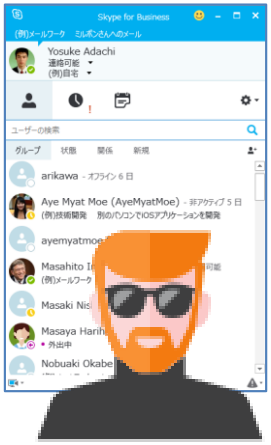
Office 365

ログが残っても問題発生後に該当のログを探す必要がある。

情報漏洩の危険性を残しながらの運用

外部接続利用時の危険性

外部接続（外部フェデレーション）を実施される場合、完全にログが残らない形で、ファイル内容の閲覧が可能になる利用パターンが明確に存在しています。



社外ユーザ

個人が無料もしくは安価にOffice365を契約しての利用が可能

外部ユーザは社内ユーザの会社名、組織名、名前、SIPアドレス、メールアドレスも取得できます。

外部接続

コンプライアンス違反

明日発表予定の決算報告書

申請前の特許情報

特定の個人の契約情報

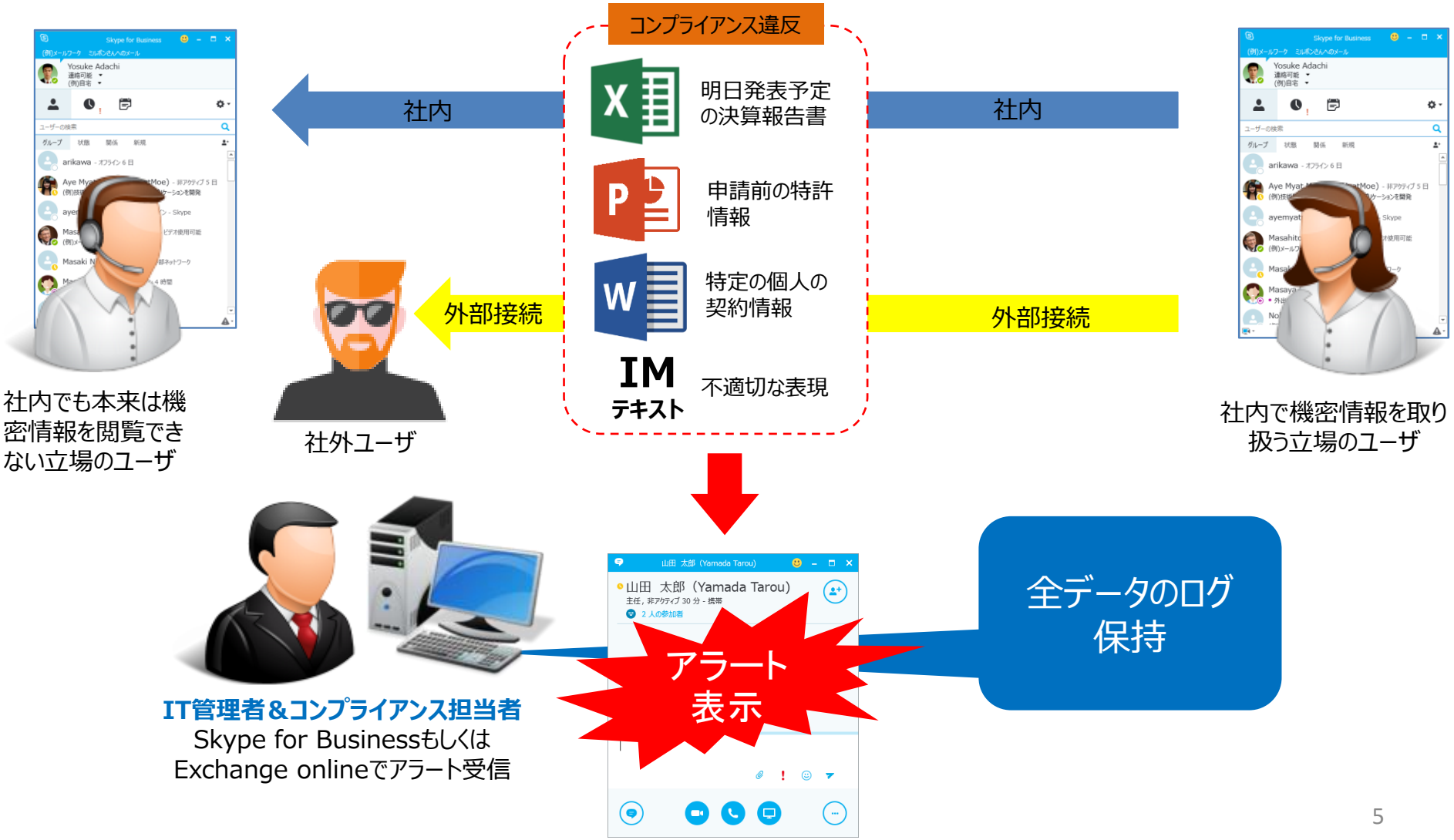
外部接続

社内で機密情報を取り扱う立場のユーザ

日本企業のほとんどが、この事実を知らずにSkype for Businessを運用しています。

Skype for Business コンプライアンスガードの特徴

- Skype for Business Server / Onlineのコンプライアンス機能では網羅していない利用パターンの全てのログ、スクリーンショット、録音の取得を行い、ユーザの利用を監視し続けます。
- リアルタイムでIMのメッセージ内容、ファイル名の監視しつづけ、不適切な内容が発見された段階でIT管理者やコンプライアンス担当者にSkype for BusinessもしくはExchangeにてアラートします。



Skype for Businessには、下記のような情報漏洩対策の限界があります。

Office 365 Skype for Business Onlineの限界

- インプレースホールドと訴訟ホールド機能では、問題の事実発生後に、日付、差出人ユーザ、受信ユーザ、キーワードを設定して該当するセッション（会話・会議）を検索・発見する必要があります。

- 下記はインプレースホールドの対象外であり、トラックすることが出来ません。
  - 1対1（ P2P ）および会議の音声・映像通話
  - 1対1（ P2P ）および会議のデスクトップの表示 / プログラムの表示
  - 1対1（ P2P ）および会議のホワイトボード、投票、質疑応答
  - 1対1（ P2P ）でのファイルの送信（受信）したファイルの実体。
  - 参照URL：https://blogs.msdn.microsoft.com/lync_support_team_blog_japan/2017/02/16/sfbo-archive/

Skype for Business Serverの限界

- 「アーカイブ」（保持）と呼ばれる機能があるもの下記各項目がアーカイブ（保持）されません。
  - 1対1（ P2P ）のファイル転送
  - 1対1（ P2P ）のインスタント メッセージおよび会議の音声/ビデオ
  - 1対1（ P2P ）のインスタント メッセージおよび会議のアプリケーション共有
  - 会議のコメント
  - 参照URL： https://technet.microsoft.com/ja-jp/library/dn951419.aspx

※　上記内容は2017年4月23日時点の調査内容です。Online、Serverともアップデートにより上記の内容が改修される可能性があります。

Office 365 インプレースホールドでログが取得可能な範囲

#	項目	会議 Skype for Business Client （社内）to（社内）、（社内）to（社外） WebApp（社内）to（社外）		1対1（P2P） SfB Client（社内）	
		可否	備考	可否	備考
1	IM テキスト	○	-	○	-
2	セッション参加者	○	-	○	-
3	音声通話	○	セッション開始・終了時刻は記録可能	○	セッション開始・終了時刻
4	ビデオ通話	○	セッション開始・終了時刻は記録可能	○	セッション開始・終了時刻
5	ファイルの転送（送信）	-	会議には当機能は存在しない。正確には「添付ファイルの追加」が機能として存在している。	△	ファイル名は取得可能であるが、ファイルの実体は残らない。
6	デスクトップの表示	×	セッション開始・終了時刻は取得可能であるが、表示しているファイルのファイル名が取得不可	×	セッション開始・終了時刻は取得可能であるが、表示しているファイルのファイル名が取得不可
7	デスクトップの表示の制御を渡す	×	一切ログが残らない。制御を渡したユーザのPCの内部まで確認可能となり、制御を渡したユーザの権限で操作できてしまう。	×	一切ログが残らない。制御を渡したユーザのPCの内部まで確認可能となり、制御を渡したユーザの権限で操作できてしまう。
8	プログラムの表示	×	セッション開始・終了時刻は取得可能であるが、表示しているファイルのファイル名が取得不可	×	セッション開始・終了時刻は取得可能であるが、表示しているファイルのファイル名が取得不可
9	プログラムの表示の制御を渡す	×	一切ログが残らない。	×	一切ログが残らない。
10	PowerPointファイルの表示	○	ファイル名・ファイルの実体	-	P２P無し
11	添付ファイルの追加	○	ファイル名・ファイルの実体	-	1対1（P2P）には当機能は存在しない。正確には「ファイルの転送（送信）」が存在している。
12	共有のメモ	-	-	-	-
13	個人のメモ	-	-	-	-
14	ホワイトボードの表示	△	ファイル名は取得可能。ファイルの実体は暗号化されていてひらけない。	-	P２P無し
15	投票	△	ファイル名は取得可能。ファイルの実体は暗号化されていてひらけない。	-	P２P無し
16	質疑応答	○	テキストファイルとして内容が保存される。	-	P２P無し

参照： https://blogs.msdn.microsoft.com/lync_support_team_blog_japan/2017/02/16/sfbo-archive/

Lync Server 2013のアーカイブ機能で取得可能なログ

項目	会議 Skype for Business Client （社内）to（社内）、（社内）to（社外） WebApp（社内）to（社外）		1対1（P2P） SfB Client（社内）	
	可否	備考	可否	備考
IM テキスト	○	-	○	-
セッション参加者	○	-	○	-
音声通話	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり
ビデオ通話	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり
ファイルの転送（送信）	-	会議には当機能は存在しない。正確には「添付ファイルの追加」が機能として存在している。	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり
デスクトップの表示	×	セッション開始・終了時刻は取得可能であるが、表示しているファイルのファイル名が取得不可	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり
デスクトップの表示の制御を渡す	×	一切ログが残らない。制御を渡したユーザのPCの内部まで確認可能となり、制御を渡したユーザの権限で操作できてしまう。	×	一切ログが残らない。制御を渡したユーザのPCの内部まで確認可能となり、制御を渡したユーザの権限で操作できてしまう。
プログラムの表示	×	セッション開始・終了時刻は取得可能であるが、表示しているファイルのファイル名が取得不可	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり
プログラムの表示の制御を渡す	×	一切ログが残らない。	×	一切ログが残らない。
PowerPointファイルの表示	○	ファイル名・ファイルの実体	-	P２P無し
添付ファイルの追加	○	ファイル名・ファイルの実体	-	1対1（P2P）には当機能は存在しない。正確には「ファイルの転送（送信）」が存在している。
共有のメモ	-	-	-	-
個人のメモ	-	-	-	-
ホワイトボードの表示	△	ファイル名は取得可能。ファイルの実体は暗号化されていてひらけない。	-	P２P無し
投票	△	ファイル名は取得可能。ファイルの実体は暗号化されていてひらけない。	-	P２P無し
質疑応答	×	Microsoft社TechNetにて公開されている情報では不可。但し検証の必要あり	-	P２P無し

参照： https://technet.microsoft.com/ja-jp/library/dn951419.aspx

黄色の部分はOffice365 Skype for Business Onlineとの差異

Skype for BusinessのIM（テキストメッセージ）およびファイル転送を全てリアルタイムに監視、問題となるキーワード、ファイル名が送受信された時点でアラートを管理者に通知します。

■ キーワードを設定するだけです。

- □ IM（テキストメッセージ）でやり取りされてはいけないキーワードを設定。
- □ Skype for Businessでの共有を禁止するファイル名に含まれるキーワードを設定します。

※ ファイルの中身をスキャンする場合は別途見積もりとさせていただきます。

■ 全てのテキストメッセージ、ファイル転送、共有情報をリアルタイムでトラックします。

- □ 当システムは一般ユーザに知られることなく、全てのIM （テキストメッセージ）、ファイル転送の内容をトラックし続けます。
- □ 共有されたファイル名を全て取得することが可能です。

※ ファイルの実体を保存する場合は別途御見積とさせていただきます。

■ ビデオ通話、デスクトップ表示、プログラムの表示、PowerPointファイルの表示、ホワイトボードの表示がされている最中1分に１回、ランダムにスクリーンショットを取得し続けます。

■ 音声通話とビデオ通話がされている最中、10分間に30秒、ランダムに録音を行います。

■ アラートの発生

- □ Skype for Business、Exchangeの機能を利用して禁止キーワードが発生した時点でIT管理者にアラートを送信します。

※ またスクリーンショット、録画情報、録音情報を任意のSQLサーバにアップロードさせることが可能です。別途見積もりとさせていただきます。

ログ取得もしくは保存できる内容

- ログの対象
  - デスクトップの表示
  - アプリケーションの表示
  - PowerPointの表示
  - ホワイトボード
  - 添付ファイルの追加（ファイルの送信）
  - その他(ホワイトボード、投票、質疑応答)
  - （IM上からの）ファイルの送信
  - 音声通話
  - ビデオ通話

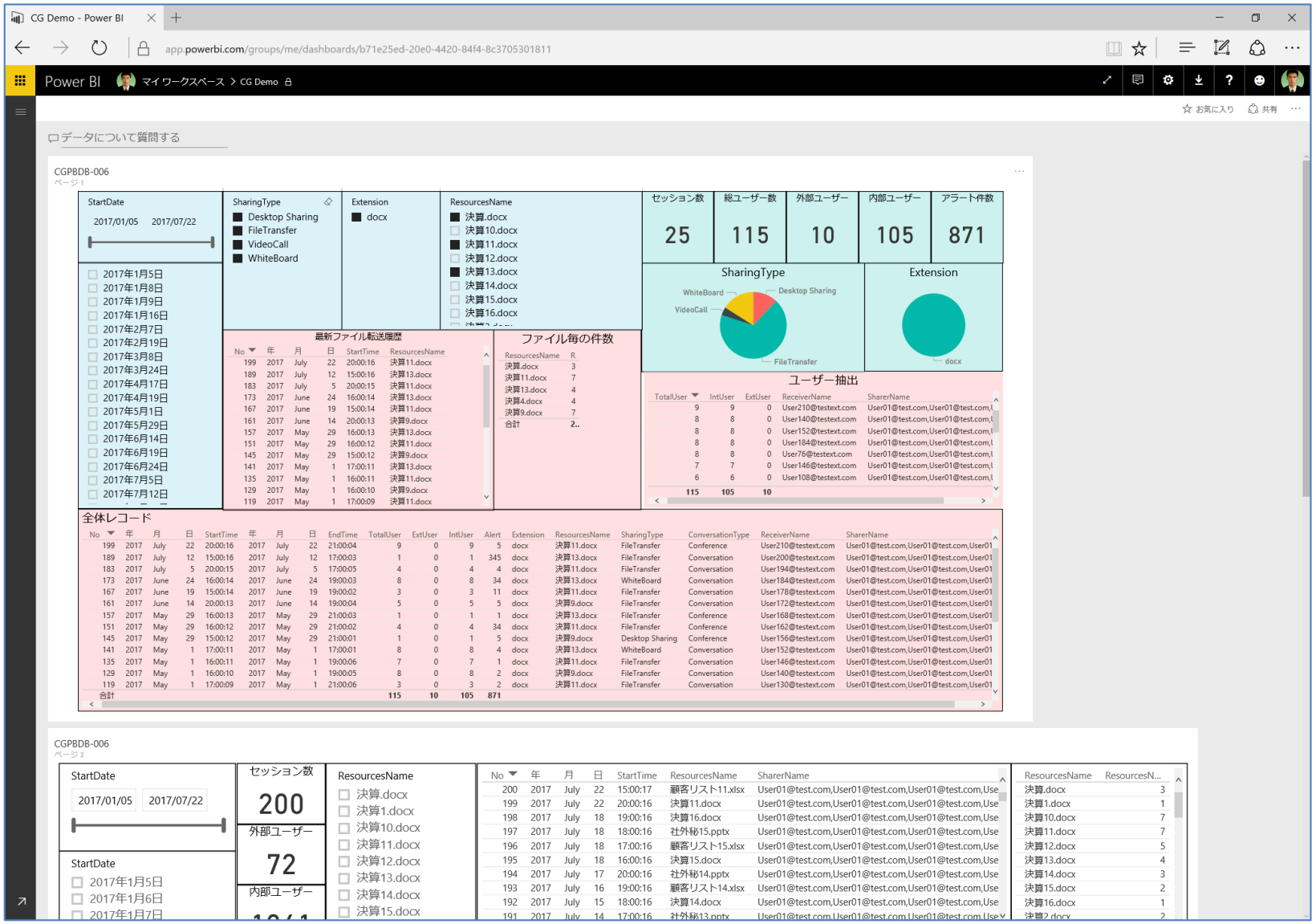
- 音声ファイルの取得（保存）の対象
  - 音声通話
  - ビデオ通話
    - 10分間に30秒、ランダムに録音
    - VoiceRecordingのファイル名：Tarou Yamada(sip:demo@fairuse.jp)_yyyyMMdd_hhmmss_yyyyMMdd_hhmmss.wav
      ※アップロードしている本人のDisplayNameとログインID

- スクリーンショットの取得（保存）の対象
  - ビデオ通話
  - デスクトップ表示
  - プログラムの表示
  - PowerPointファイルの表示
  - ホワイトボードの表示
  - 投票
  - 質疑応答
    - 1分に１回ランダム
    - スクリーンショットのファイル名： Tarou Yamada(sip:demo@fairuse.jp)_yyyyMMdd_hhmmss.png
      ※送信者のDisplayNameとログインID

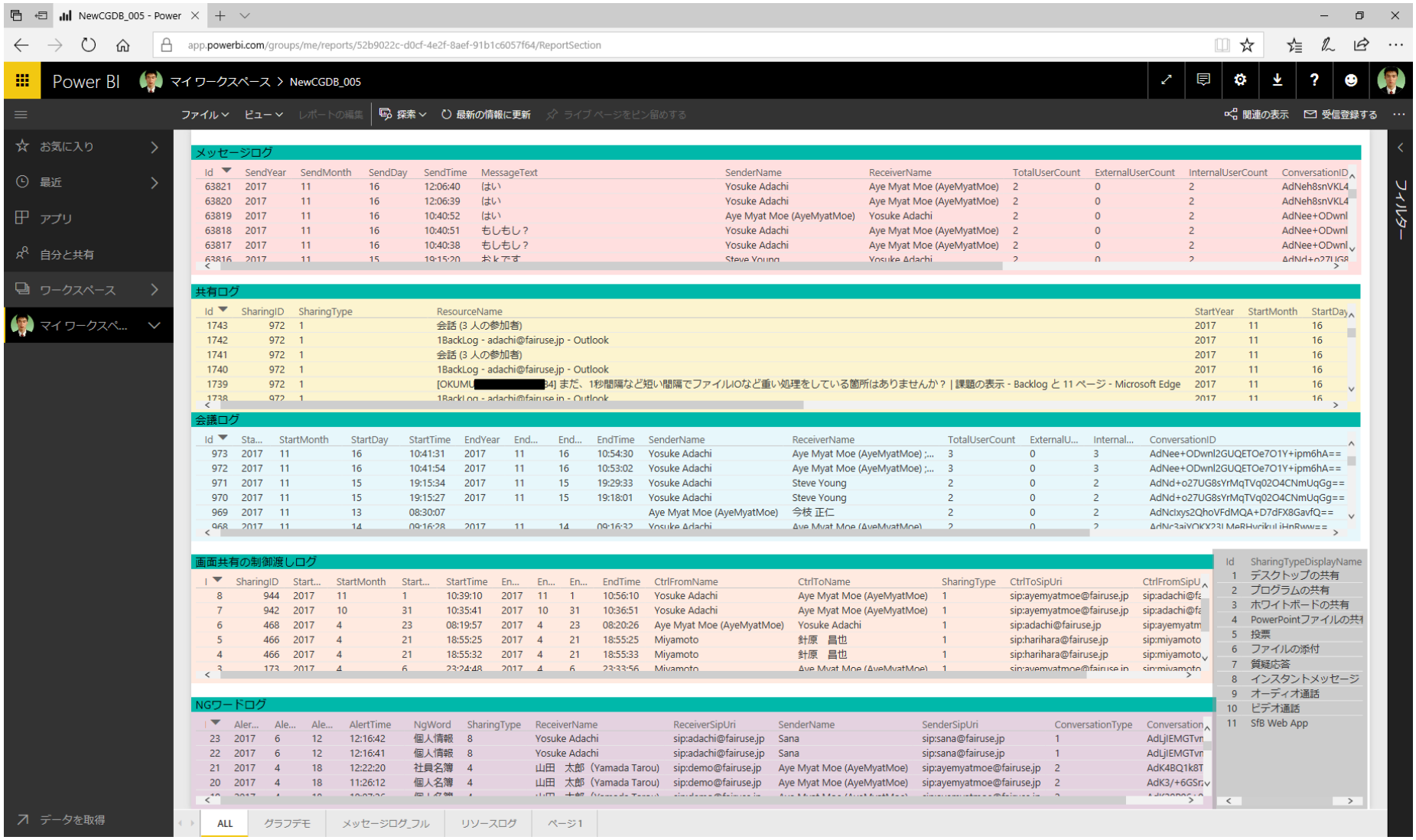
※　上記は全てハードコーディングでOn/Offの設定が可能です。つまり、各企業ごとに必要なログの取得だけを実施します。

PowerBIを用いたログ内容のインターフェース①

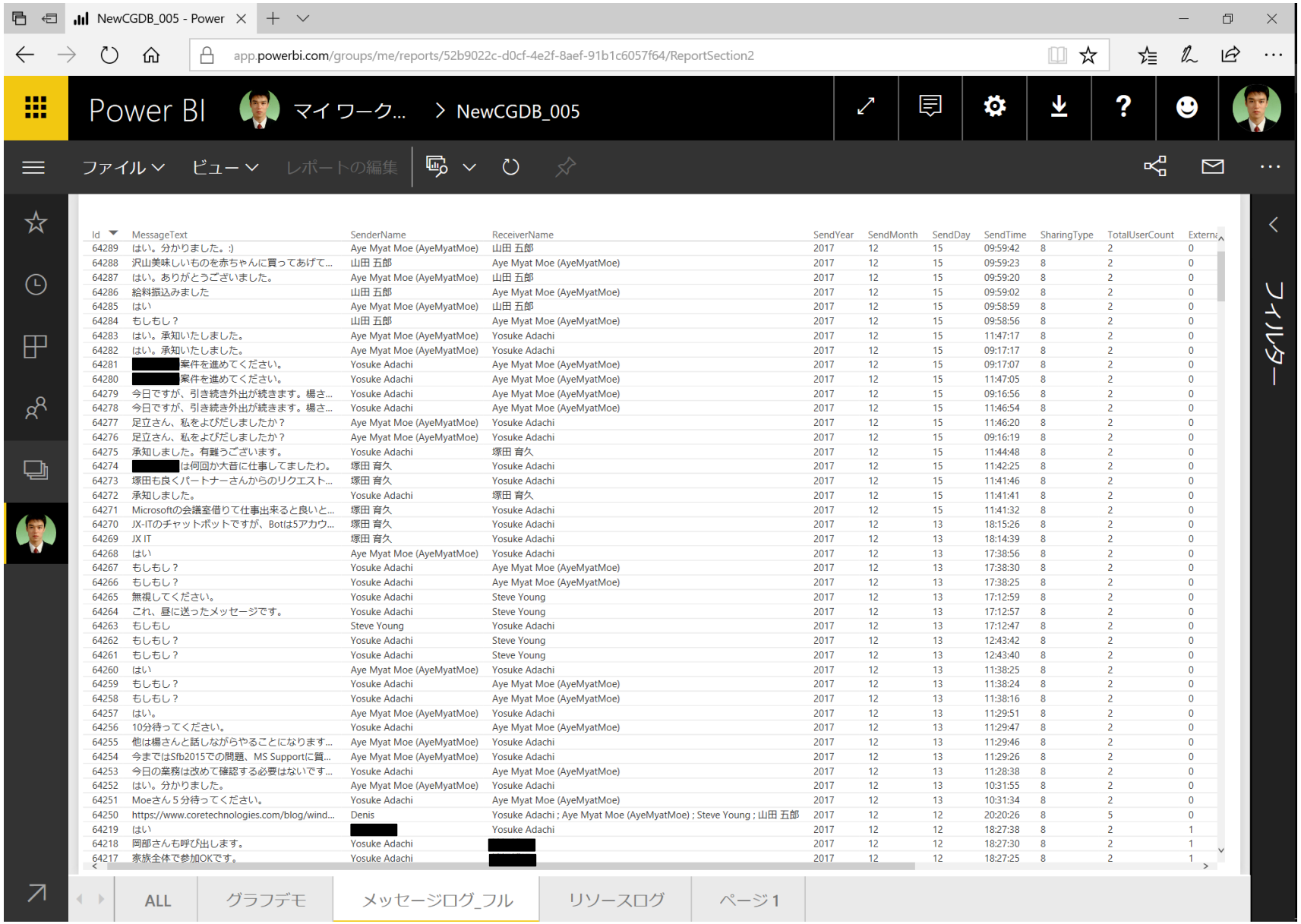
MicrosoftのPowerBIを用いてログ表示を行うことも可能です。



PowerBIを用いたログ内容のインターフェース②

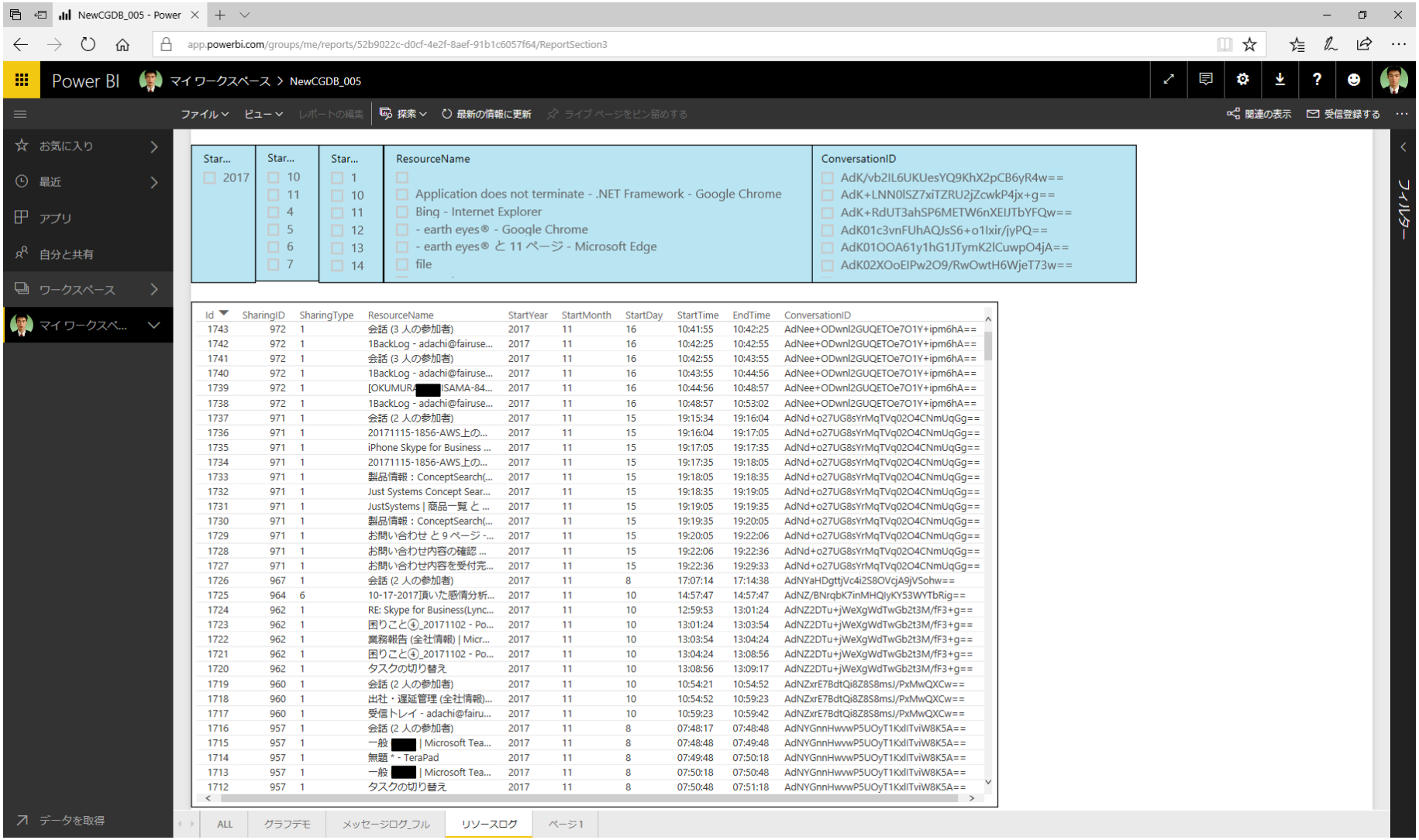


PowerBIを用いたログ内容のインターフェース③



Id	MessageText	SenderName	ReceiverName	SendYear	SendMonth	SendDay	SendTime	SharingType	TotalUserCount	Externa
64289	はい。分かりました。:)	Aye Myat Moe (AyeMyatMoe)	山田 五郎	2017	12	15	09:59:42	8	2	0
64288	沢山美味しいものを赤ちゃんに買ってあげて...	山田 五郎	Aye Myat Moe (AyeMyatMoe)	2017	12	15	09:59:23	8	2	0
64287	はい。ありがとうございました。	Aye Myat Moe (AyeMyatMoe)	山田 五郎	2017	12	15	09:59:20	8	2	0
64286	給料振込みました	山田 五郎	Aye Myat Moe (AyeMyatMoe)	2017	12	15	09:59:02	8	2	0
64285	はい	Aye Myat Moe (AyeMyatMoe)	山田 五郎	2017	12	15	09:58:59	8	2	0
64284	もしもし？	山田 五郎	Aye Myat Moe (AyeMyatMoe)	2017	12	15	09:58:56	8	2	0
64283	はい。承知いたしました。	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	15	11:47:17	8	2	0
64282	はい。承知いたしました。	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	15	09:17:17	8	2	0
64281	[redacted]案件を進めてください。	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	15	09:17:07	8	2	0
64280	[redacted]案件を進めてください。	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	15	11:47:05	8	2	0
64279	今日ですが、引き続き外出が続きます。楊さ...	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	15	09:16:56	8	2	0
64278	今日ですが、引き続き外出が続きます。楊さ...	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	15	11:46:54	8	2	0
64277	足立さん、私をよびだしましたか？	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	15	11:46:20	8	2	0
64276	足立さん、私をよびだしましたか？	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	15	09:16:19	8	2	0
64275	承知しました。有難うございます。	Yosuke Adachi	塚田 育久	2017	12	15	11:44:48	8	2	0
64274	[redacted]は何回か大昔に仕事してましたわ。	塚田 育久	Yosuke Adachi	2017	12	15	11:42:25	8	2	0
64273	塚田も良くパートナーさんからのリクエスト...	塚田 育久	Yosuke Adachi	2017	12	15	11:41:46	8	2	0
64272	承知しました。	Yosuke Adachi	塚田 育久	2017	12	15	11:41:41	8	2	0
64271	Microsoftの会議室借りて仕事出来ると良いと...	塚田 育久	Yosuke Adachi	2017	12	15	11:41:32	8	2	0
64270	JX-ITのチャットボットですが、Botは5アカウ...	塚田 育久	Yosuke Adachi	2017	12	13	18:15:26	8	2	0
64269	JX IT	塚田 育久	Yosuke Adachi	2017	12	13	18:14:39	8	2	0
64268	はい	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	13	17:38:56	8	2	0
64267	もしもし？	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	17:38:30	8	2	0
64266	もしもし？	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	17:38:25	8	2	0
64265	無視してください。	Yosuke Adachi	Steve Young	2017	12	13	17:12:59	8	2	0
64264	これ、昼に送ったメッセージです。	Yosuke Adachi	Steve Young	2017	12	13	17:12:57	8	2	0
64263	もしもし	Steve Young	Yosuke Adachi	2017	12	13	17:12:47	8	2	0
64262	もしもし？	Yosuke Adachi	Steve Young	2017	12	13	12:43:42	8	2	0
64261	もしもし？	Yosuke Adachi	Steve Young	2017	12	13	12:43:40	8	2	0
64260	はい	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	13	11:38:25	8	2	0
64259	もしもし？	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	11:38:24	8	2	0
64258	もしもし？	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	11:38:16	8	2	0
64257	はい。	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	13	11:29:51	8	2	0
64256	10分待ってください。	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	11:29:47	8	2	0
64255	他は楊さんと話しながらやることになります...	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	13	11:29:46	8	2	0
64254	今まではSfb2015での問題、MS Supportに質...	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	13	11:29:26	8	2	0
64253	今日の業務は改めて確認する必要はないです...	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	11:28:38	8	2	0
64252	はい。分かりました。	Aye Myat Moe (AyeMyatMoe)	Yosuke Adachi	2017	12	13	10:31:55	8	2	0
64251	Moeさん５分待ってください。	Yosuke Adachi	Aye Myat Moe (AyeMyatMoe)	2017	12	13	10:31:34	8	2	0
64250	https://www.coretechnologies.com/blog/wind...	Denis	Yosuke Adachi ; Aye Myat Moe (AyeMyatMoe) ; Steve Young ; 山田 五郎	2017	12	12	20:20:26	8	5	0
64219	はい	[redacted]	Yosuke Adachi	2017	12	12	18:27:38	8	2	1
64218	岡部さんも呼び出します。	Yosuke Adachi	[redacted]	2017	12	12	18:27:30	8	2	1
64217	家族全体で参加OKです。	Yosuke Adachi	[redacted]	2017	12	12	18:27:25	8	2	1

PowerBIを用いたログ内容のインターフェース④



Skype for Business WebAppにおける問題点

Skype for Business WebAppの参加者管理の問題点

- 会議URLを送信して開催の場合、不特定多数が参加出来てしまいます。
  - ◆外部接続（外部フェデレーション）を認めている場合は、外部の不特定多数のユーザが参加出来てしまいます。
  - ◆外部接続にて仮想ロビー上にて、主催者が承認する場合でも、参加者の身元を特定することが困難です。
  - ◆社内でも会議URLを知ったユーザが任意で参加することが可能になります。

Skype for BusinessにないCisco社のWebExの利点

- 運用上、会議参加者を事前に登録し、その参加者に対してメールを送信して参加を促すことが可能です。

コンプライアンスガード　参加者チェック機能

- 弊社のコンプライアンスガードでは、事前に登録されたユーザ以外の参加者を制限することが可能です。参加した場合には会議から自動的に追い出します。（2018年6月末リリース予定：オプション機能ライセンス購入が必要）

弊社紹介

弊社紹介

1. 弊社代表の足立洋介がMicrosoft MVPをOffice Server and Services分野にて受賞。

※Microsoft MVPとはMicrosoft社外で最も優れたエンジニアに表彰される称号です。

※Office Server and ServicesはOffice 365、Exchange、SharePoint、Skype for Business (Lync)の製品群を指します。

2. Microsoft社のLyncに関する国内最大のイベントLync Interact Japan2014にて弊社製品のWork Time Recorderがメインセッションにて紹介を受ける。

http://www.microsoft.com/ja-jp/lync/interact/default.aspx

3. ワークスタイル変革 Day 2014のMicrosoft社の「ワークスタイル変革」への取り組みのセッションにて弊社の製品Lync IoTの紹介をいただく。

http://www.ric.co.jp/expo/wsd2014/program.html

4. Microsoft社の製品を取り扱う大手Sierばかりが一同に会するクローズドなイベントであるLync Partner Dayのジェネラルセッションにて弊社代表の足立洋介が講演の機会をいただく。

http://www.slideshare.net/adachiyosuke/lync-developerday2014

5. 2017年5月23日、24日開催のMicrosoft社の開発会社、SIer向けのイベントであるde:codeにて、日本マイクロソフトのマーケティング部門の御依頼により、ブース出展とセミナーでのデモをいただくことが確定。（ブース出展は通常はスポンサー料金が必要であるが、弊社だけ特別御協力出展。）

https://www.microsoft.com/ja-jp/events/decode/2017/

弊社概要

フェアユース株式会社概要

- 2010年11月に会社設立
- 代表取締役　足立洋介
- SharePoint のiOS、Androidアプリである「ShareOffice」の販売
- Skype for BusinessのAPIを利用したWindows、iOSアプリ開発
- iOS、Android、WindowsStoreアプリ等の受託開発

主要顧客企業

- KDDI株式会社
- 日本マイクロソフト株式会社
- 株式会社ミルボン
- 株式会社内田洋行(販売代理店様)
- 株式会社富士通エフサス(販売代理店様)
- 株式会社日立ソリューションズ(販売代理店様)
- NECネッツエスアイ株式会社
- ✓ 御陰様で直接取引をさせていただく東証一部上場企業が30社以上となりました。

連絡先

- 電話：03-6868-3223
- FAX ： 03-6869-1184
- メールアドレス：contact@fairuse.jp
- URL: http://www.fairuse.jp/
- 住所：〒151-0073 東京都渋谷区笹塚2-19-3 大成ビル5F

Share Office

- SharePoint、SharePoint OnlineのiPhone、iPad、Androidのネイティブアプリ
- iOS、Android、WindowsStoreの各種プラットフォーム対応
- 日本の大企業のセキュリティポリシー、ネットワークに適応するカスタマイズが可能
- http://www.fairuse.jp/shareoffice/

IoT Bot for Skype for Business

- Skype for Business上のBotが様々な質問に答えてくれます。
- Lync SDKを利用した開発
- http://www.fairuse.jp/download/IoTBot.pdf

Work Time Recorder

- テレワーク、在宅勤務向けのソリューション
- Lync SDKを利用した開発
- http://www.fairuse.jp/download/worktimerecorder.pdf

FairUSE