

ユーザー企業における
CASB を用いた
クラウド統制の実際

2019年11月27日

一般社団法人 日本クラウドセキュリティアライアンス
CASBワーキンググループ
渡辺 慎太郎(株式会社ジュピターテレコム)

会社紹介①

ケーブルテレビ事業

J:COM TV

J:COM NET

J:COM PHONE

J:COM 電力

J:COM MOBILE



ケーブルインターネットZAQのキャラクター「ざっくう」

メディア事業



会社紹介②

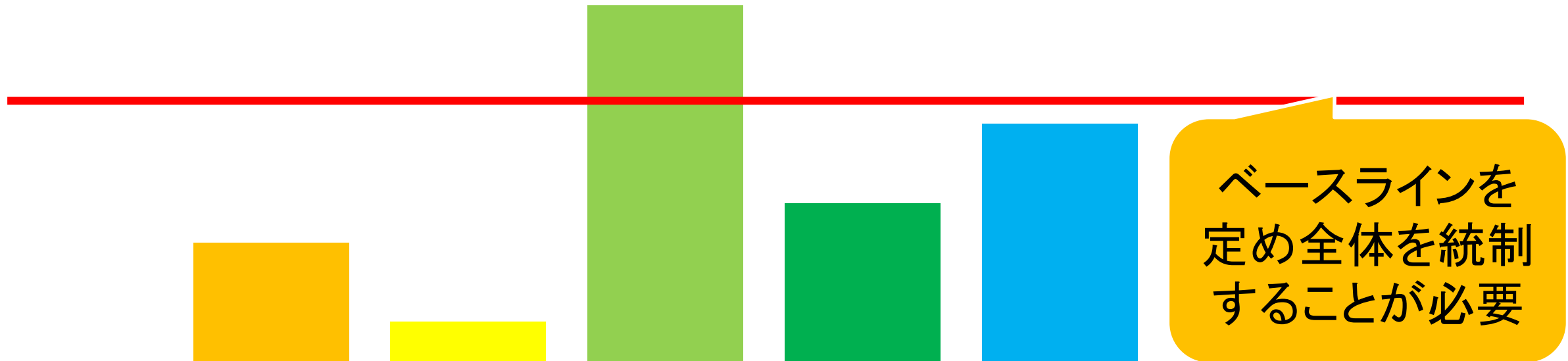
会社名	株式会社ジュピターテレコム (J:COM)
本社所在地	東京都千代田区丸の内1-8-1 丸の内トラストタワーN館
代表者	代表取締役会長 石川 雄三 代表取締役社長 井村 公彦
設立年月日	1995年1月18日
売上高	7,300億円(連結)(2018年3月期)※IFRS
従業員数	グループ総計 17,294名(2019年2月末時点)
株主	KDDI株式会社 住友商事株式会社

今日の
テーマ！

サイバーセキュリティ推進部の設立

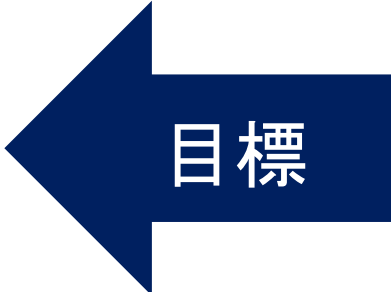
- 合併で成長したため、セキュリティレベルがまちまちだった

セキュリティ対策の度合(イメージ)



目標を決める

格付	セキュリティ対策の強度
AAAis	常時、リスクをモニタリングし、即時に柔軟な対応ができる
AAis	悪意のある内部者に対する管理策を織り込んでいる
Ais	悪意のある外部者に対する管理策を織り込んでいる
BBBis	一定の予防・防止的管理策を織り込んでいる
BBis	一定の抑止的管理策および発見的 management 策を織り込んでいる



目標

出典: アイ・エス・レーティング

- アイ・エス・レーティング社の情報セキュリティ格付を参照
- セキュリティ強度AA(内部不正の統制)を目標として設定

きょうの話題

- クラウドサービスを社内で安全に使うための仕組みづくりでCASBを格付サービスとして利用した実践例
 - 手順と体制
 - 監視の実際
- おことわり
 - 発言は個人の見解であり、所属組織を代表するものではありません
 - 本日の「クラウド」は主にSaaS/ASPを対象としており、PaaSやIaaS上のセキュア開発・運用は内容に含みません



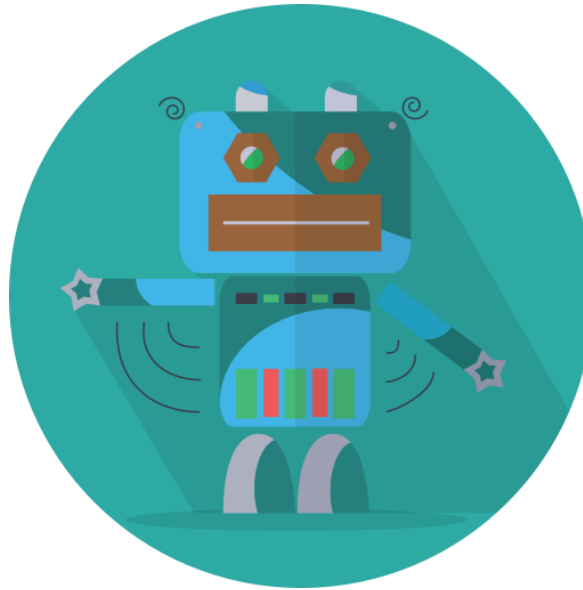
クラウド
統制
あるある

コノゴロ都ニハヤル物

DX



DevOps

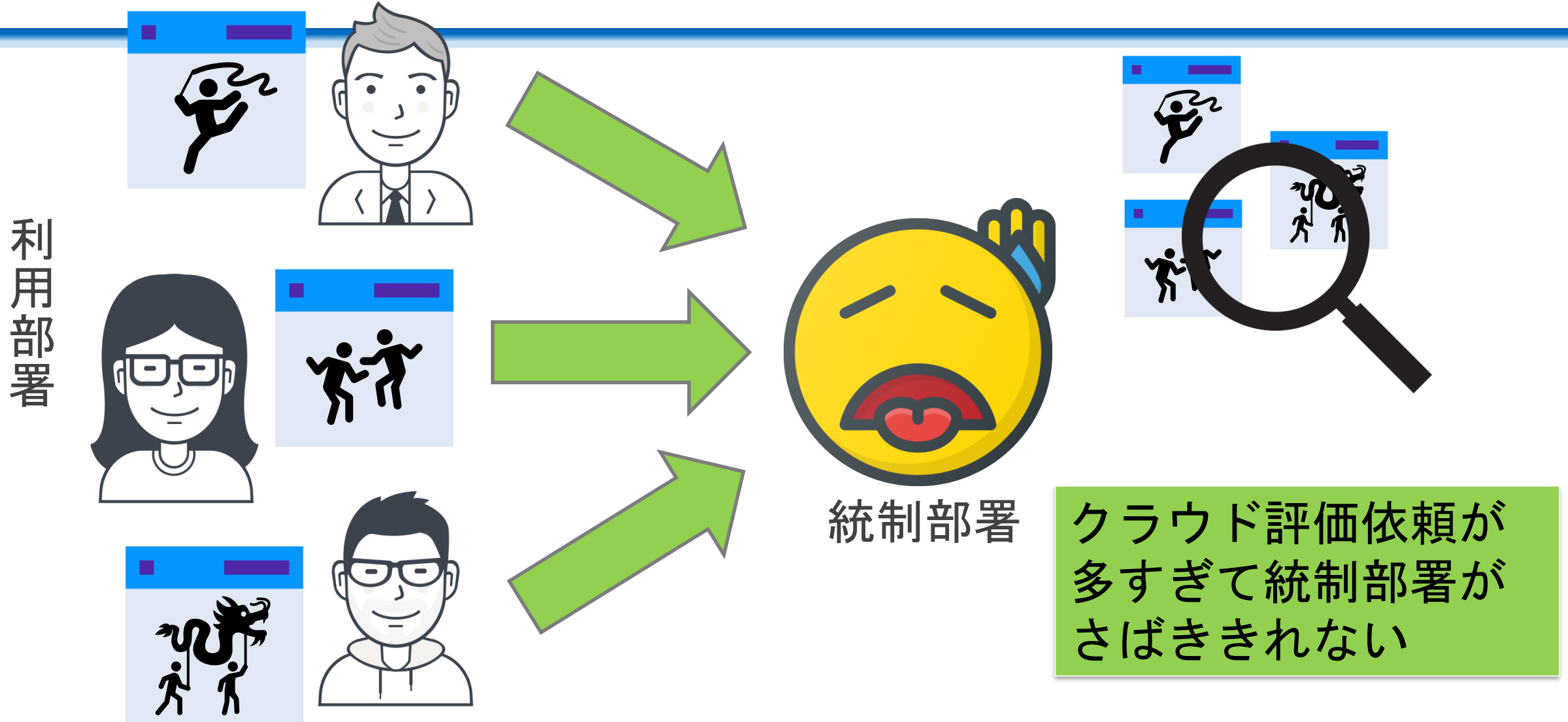


RPA

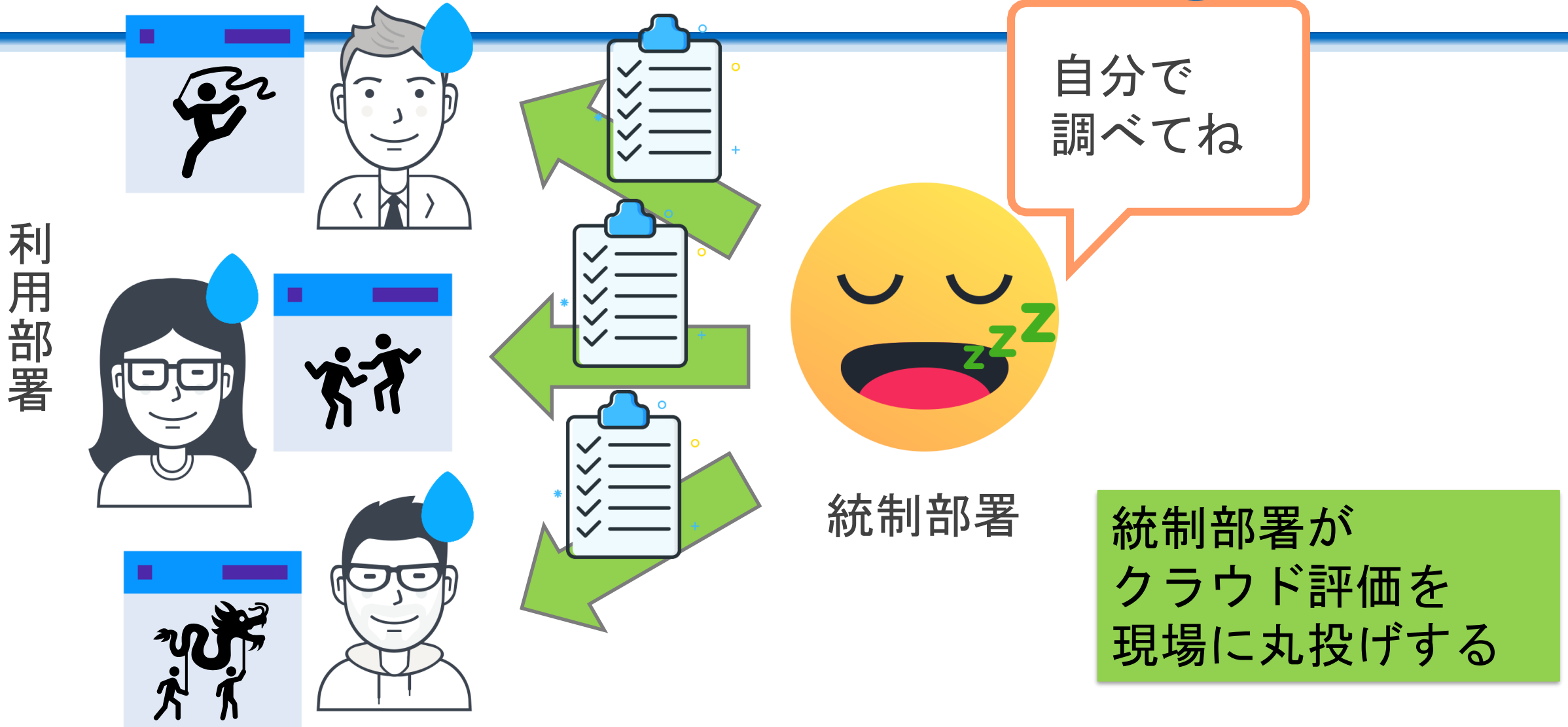


SaaS

クラウド統制の不幸なケース



クラウド統制の不幸なケース②





クラウドの 脅威と対策

クラウドの脅威源を考える

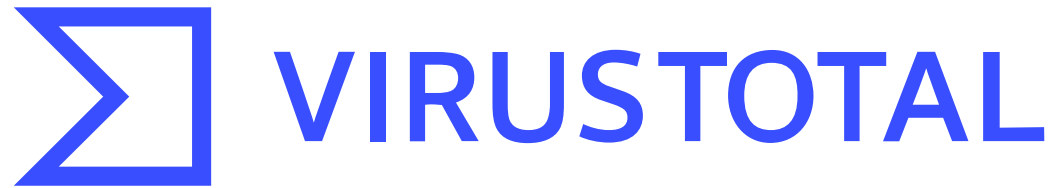
① サービス事故

- クラウド型レンタルサーバー「Zenlogicホスティング」が4日間にわたり全面停止 (IaaSの例、2018年7月)
<https://ascii.jp/elem/000/001/709/1709251/>
- 大容量ファイル送信サービス「宅ふぁいる便」における480万件の顧客情報流出 (2019年1月)
<https://ascii.jp/elem/000/001/709/1709251/>
- 平文でパスワードを管理していると思われるネット事業者が14%。
フィッシング対策協議会調べ (2019年5月)
<https://internet.watch.impress.co.jp/docs/news/1185500.html>

クラウドの脅威源を考える

- ① サービス事故
- ② 利用者の不適切使用 (abuse)

- 風呂敷残業
- 退職者によるログイン
- 不用意な露出



ウイルスチェックのつもりで情報漏えい？
VirusTotalの使い方に注意

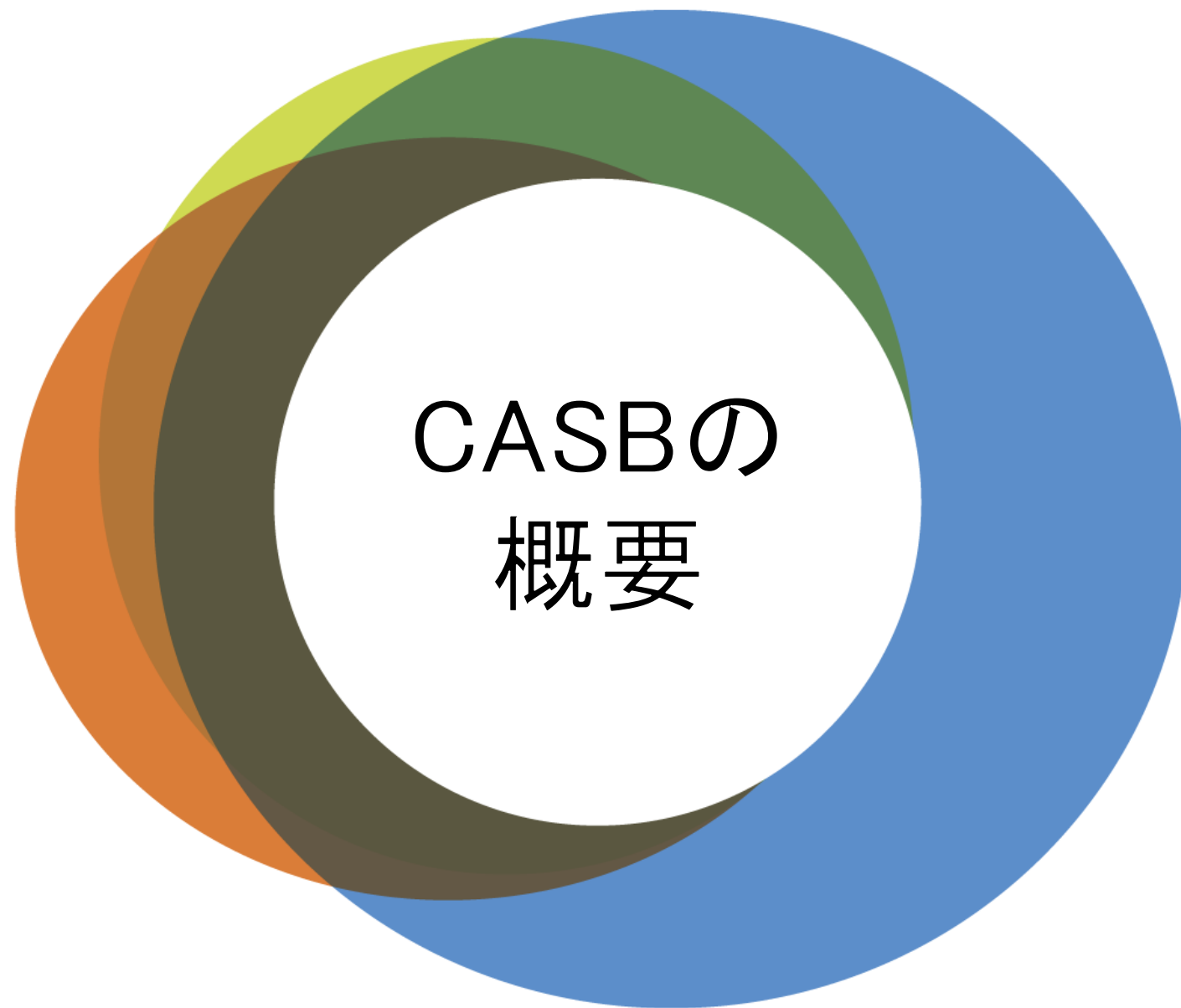
<https://www.itmedia.co.jp/enterprise/articles/1603/14/news104.html>

どんな手を打つか？

➤ クラウドサービスの脅威への対策例

	①サービス事故	②不適切使用
事前規制	格付に基づく選別	ID連携の強制
事後チェック	格付変化の追跡	未届け利用の発見 アップロードの監視

CASBが役に立つ領域



CASBの 概要

CASBとは？

- Cloud Access Security Brokerの略
- 2012年にガートナー社が提唱した技術分野

企業が利用するクラウド・アプリケーションについて
①可視化、②データ・プロテクション、③ガバナンスを
実現するサービス／製品

<https://www.sbbit.jp/article/cont1/34870>

- 2016年2月にCASB WG発足
WG主査：上田光一氏（マクニカネットワークス株式会社）

可視化の一例

Vulnerable Storage Accessed by Users

Last Updated Oct 21, 2019, 00:00 AM UTC

S3 Buckets with Open Permissions Found in Log Files

[View 30-Day History](#)

Impacted Users

Last 30 day

S3 Buckets with Open Permissions Found in Log Files

3 Storage Resources

All Vulnerabilities

Actions

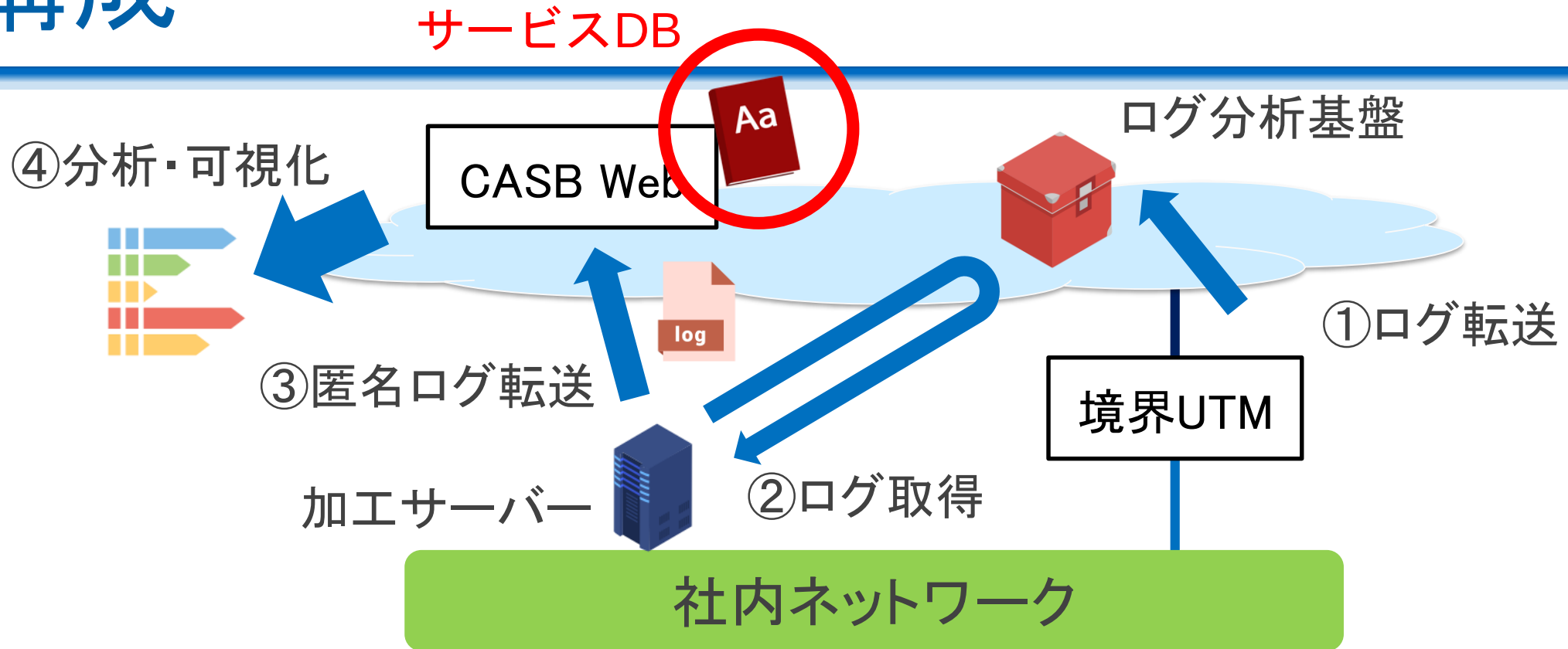


Secure Your AWS Account

Writable by ACL Modifiable by

☐	Name	Public	Users	Public	Users	Outbound Data	Inbound Data	Users	Access Count
☐	samurai-clip-media	✓		✓		8 MB	321 MB	197	361
☐	leaves-images	✓		✓		8.8 MB	339 MB	107	598
☐	ol-ent-production	✓		✓		18.2 MB	305.6 MB	728	3,840

構成



- CASBは我々よりもクラウドサービスに詳しい
→ クラウドサービスに関する情報を供給



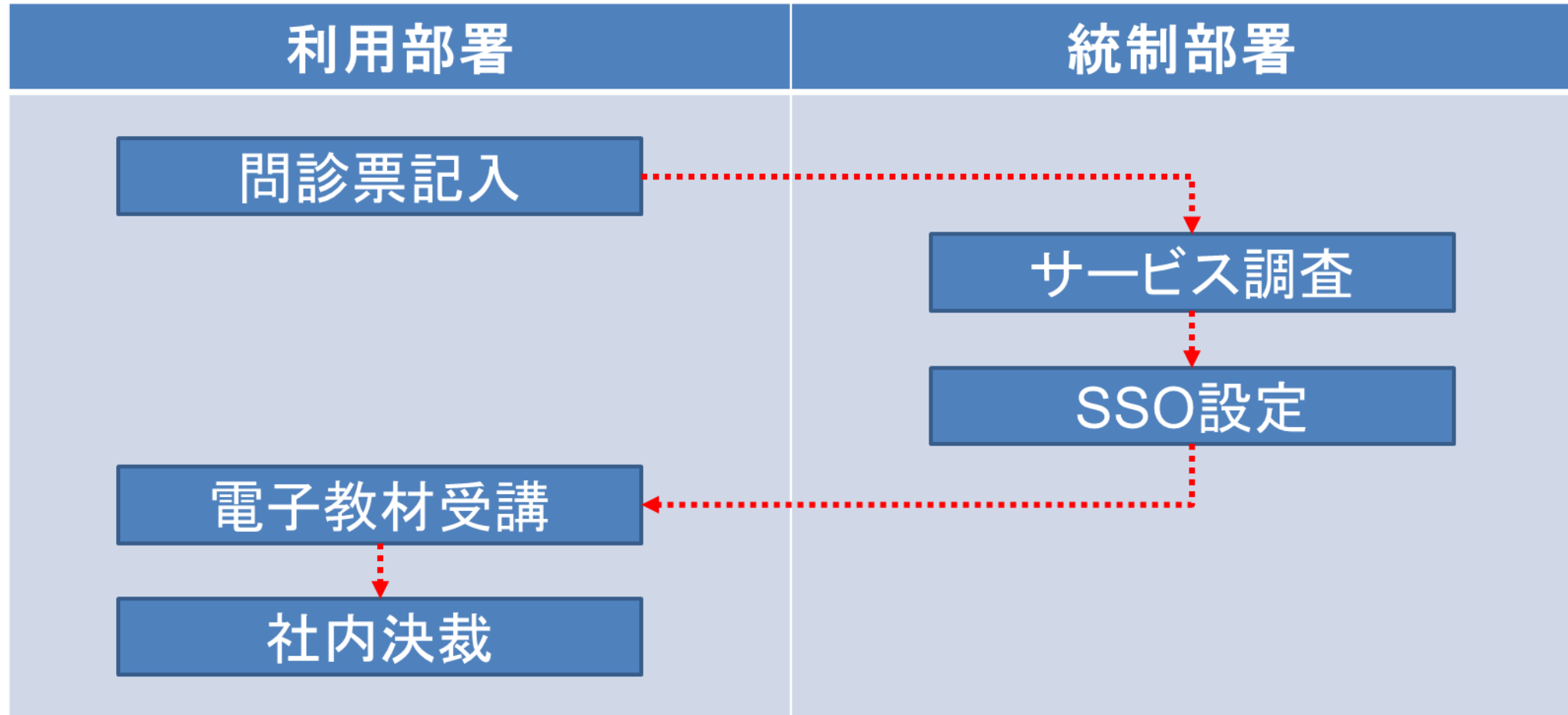
クラウド
利用開始まで

どんな手を打つか？（再掲）

➤ クラウドサービスの脅威への対策例

	①サービス事故	②不適切使用
事前規制	格付に基づく選別	ID連携の強制
事後チェック	格付変化の追跡	未届け利用の発見 アップロードの監視

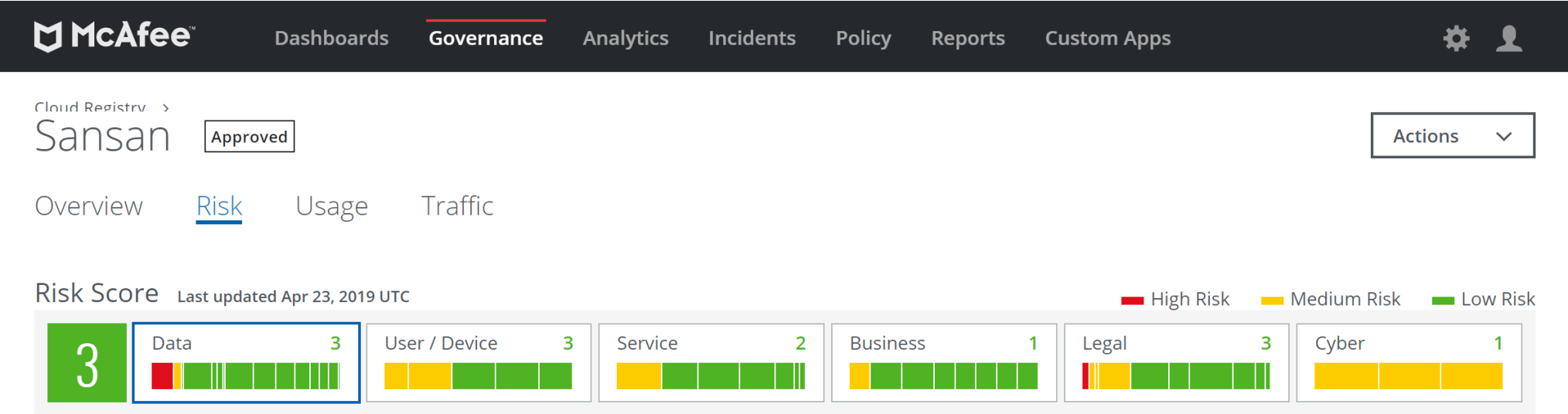
利用開始までのフロー（正常系）



問診票 → サービス調査 → SSO設定 → 電子教材受講

- 予防接種を手本にする
 - 20問以内にする
 - 選択式にする
 - 選択肢に「不明」を入れる
- 問診票はワークフローに載せる
 - Excelはやめましょう

問診票 → サービス調査 → SSO設定 → 電子教材受講



Data Risk: 3

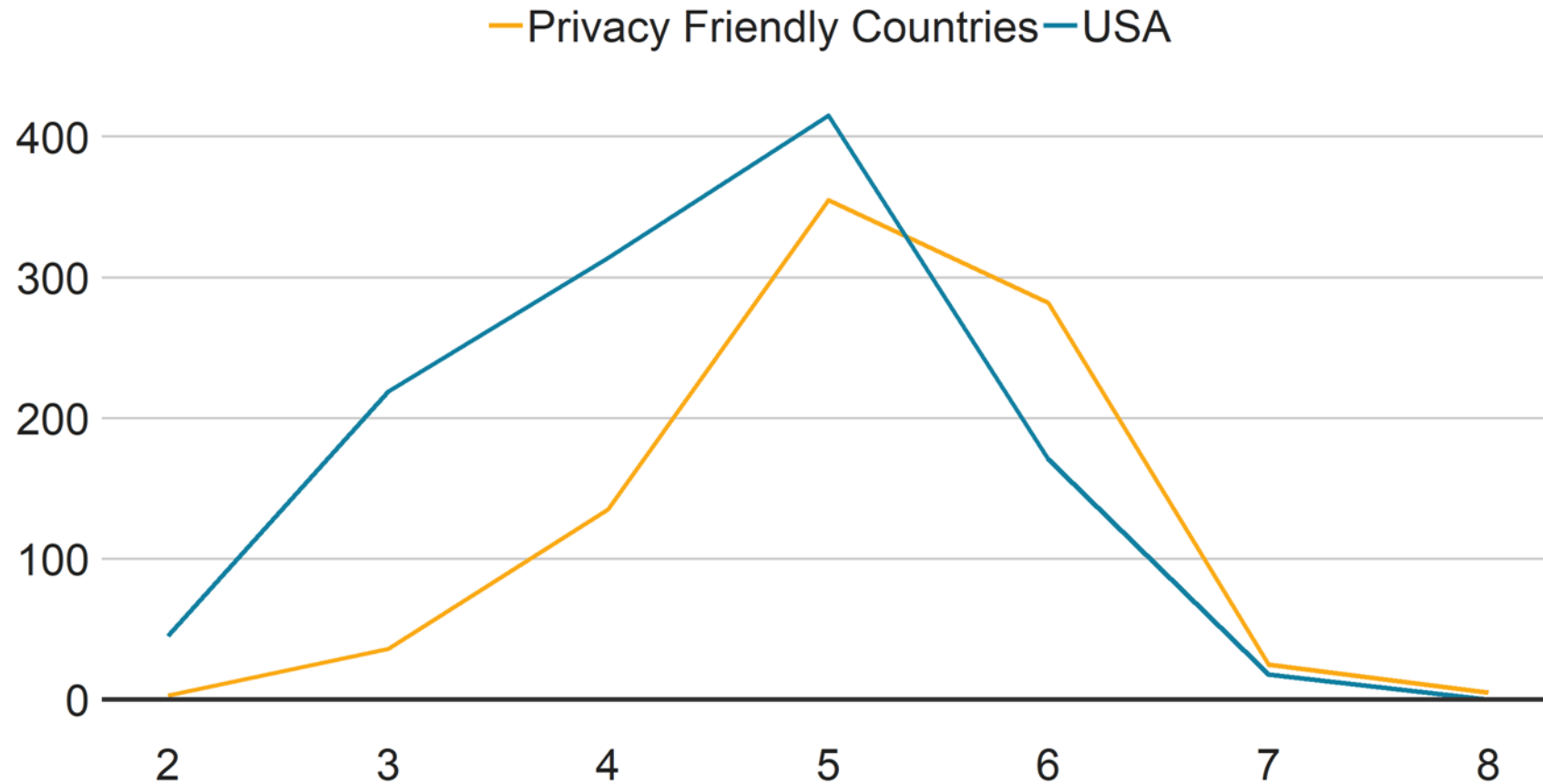
	Category	Attribute	Value	↓ Score	Attribute Weight	Weighted Score	Review Date	Notes
>	 Data Sharing	File Sharing Support	 Yes	80	12%	30	Apr 2019	+
>	 Data Loss Protection	Integrated Data Loss Prevention C	 No	60	4%	10	Apr 2019	+
>	 Encryption	Signature Algorithm of SSL Certifi	 SHA256 With RSA En...	30	1%	1	Apr 2019	+
>	 Data Retention	Data Retention Policy Upon Accou	 15 to 30 days	20	15%	11	Apr 2019	+
>	 Encryption	Data Encryption in Transit	 TLS 1.0	20	3%	2	Apr 2019	+

- CASB事業者の資源を活用する
 - 台帳に載っていないサービスは即座にリクエスト
 - リクエストへの応答速度が選定の決め手の1つだった
- CASB事業者の権威を活用する
 - リスク値の悪いサービスは許可しないと宣言しておく
 - リスク値を盾にしてサービス事業者に改善を促す

参考) 日本のサービスは安全か？

Risk Score Distributions

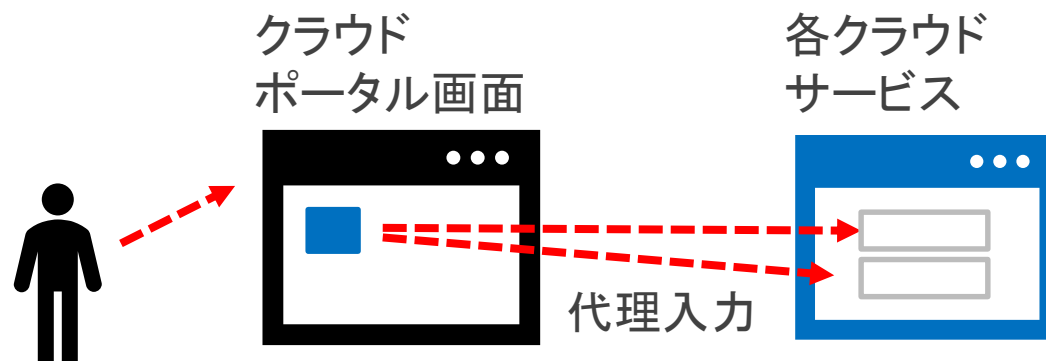
grouped by the location of Business HQ



➤ User / Device欄で、可能なID連携手法がわかる

Multi-factor Authentication	✓ Yes
Identity Federation Method	✓ SAML & OAUTH
Enterprise Identity (Integration With	✓ Yes

➤ ID連携に非対応のサービスには、フォーム代行入力で疑似的にSSOを実現(利用者にパスワードを教えない)



➤ 稟議書の起案者に電子教材の受講を義務づける

クラウドサービスを
安全に使うために

もっと、あなたに喜ぶこと。
J:COM

学ぶこと

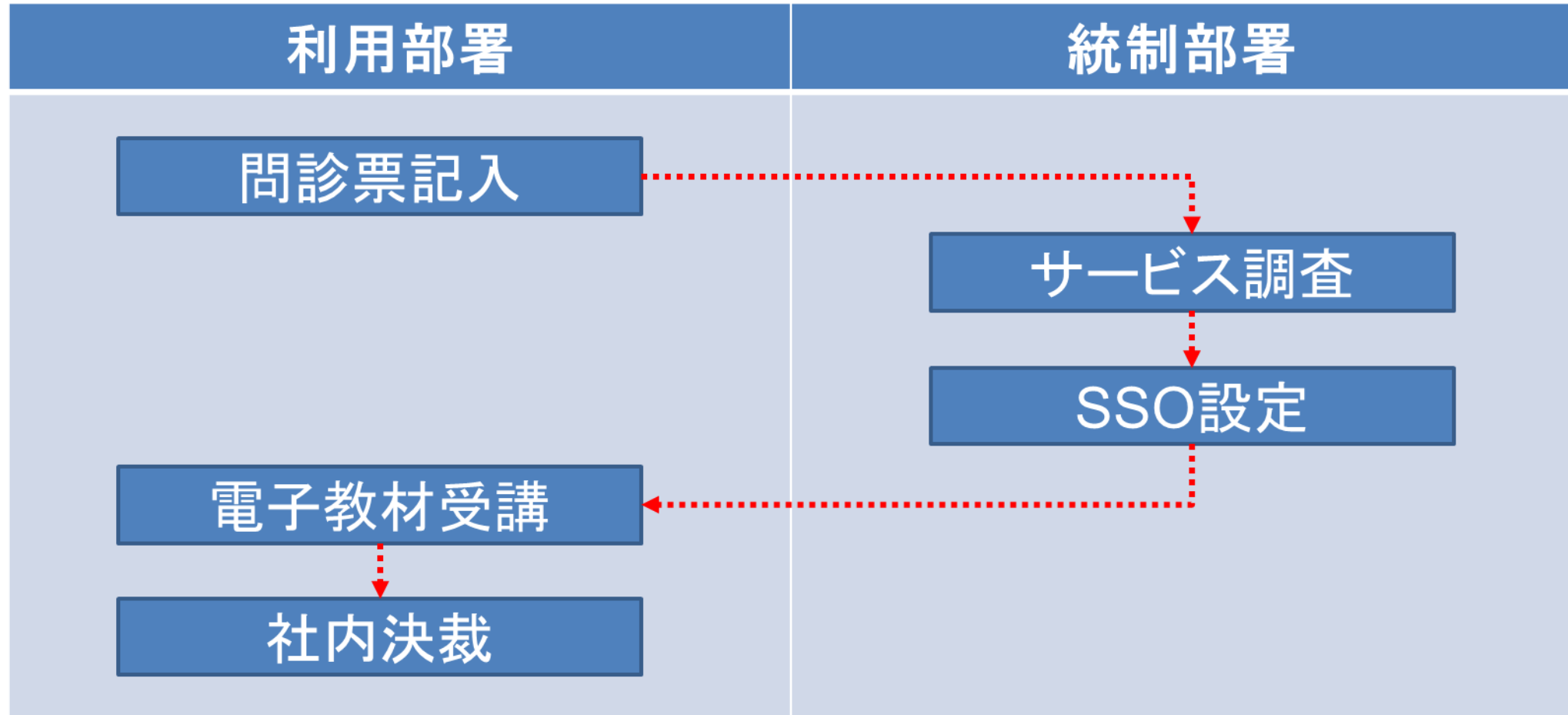
1. クラウドって何?
2. メリット
3. デメリット
4. 導入時の注意事項
5. 利用中の注意事項

時間のめやす: 約20分

ページ数: 18ページ

2018年11月1日
サイバーセキュリティ推進部
株式会社ジュピターテレコム

利用開始までのフロー（再掲）



ルールを作り、説明する

第1章 クラウドサービス利用の遵守事項	
第1条	遵守事項
第2条	クラウドサービス管理責任と役割
第3条	クラウドサービス利用のモニタリング及び停止
第2章 クラウドサービスの選定	
第4条	実施手順
第5条	クラウドサービスのテスト利用
第6条	クラウドサービスの評価
第3章 クラウドサービスの利用	
第7条	クラウドサービスの本利用
第8条	クラウドサービスの棚卸
第9条	クラウドサービスの契約終了

定着を見るため
内部監査の
質問項目に
加えてもらう

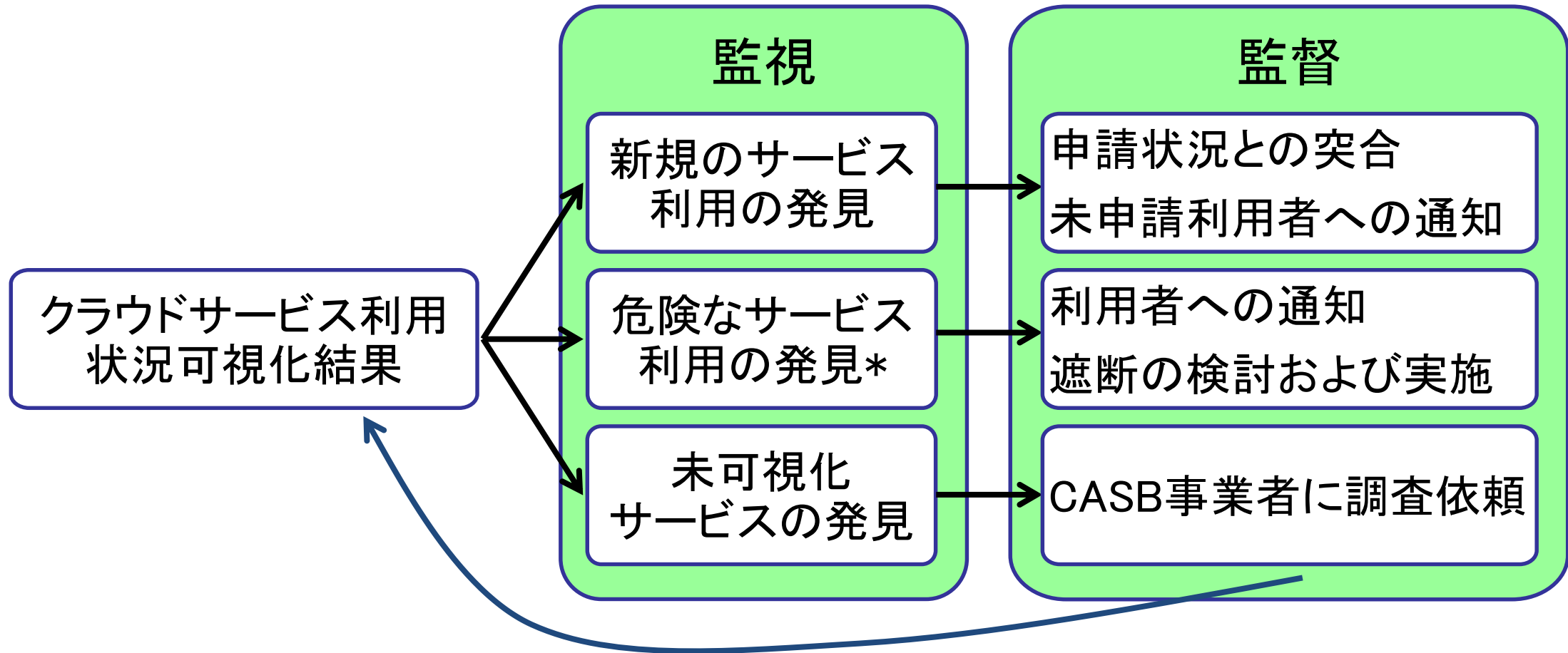


利用開始
その後の運用

利用開始後の運用

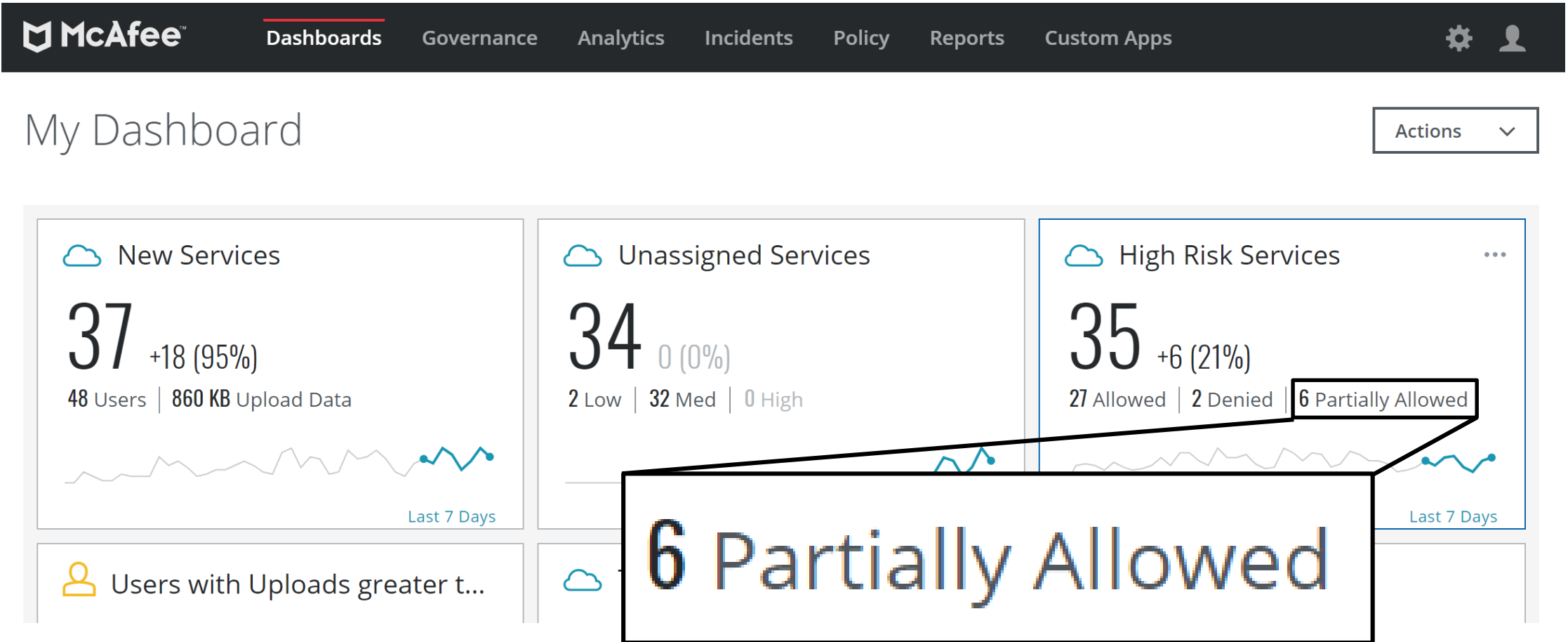
	①サービス事故	②不適切使用
事前規制	格付に基づく選別	ID連携の強制
事後チェック	格付変化の追跡	未届け利用の発見 アップロードの監視

格付変化追跡／未届け利用の発見



* 利用中に危殆化する場合も含む

新規サービス利用の発見



リスク値が変化したときに通知させる

The screenshot shows the McAfee Cloud Governance interface. At the top, there's a navigation bar with 'McAfee' logo and tabs for Dashboards, Governance, Analytics, Incidents, Policy, Reports, and Custom Apps. Below this, the 'Cloud Governance' section is active, with a toggle switch set to 'on'. The main content area is titled 'My Notifications' and includes a sub-header 'on/off Send an email notification for these Saved Views:'. A notification rule is configured with the trigger 'All Active Services' (indicated by a bell icon), the condition 'IF Risk Values', and the action '= An Increase in Risk Score & Any Change'. A callout box highlights the action text. Below the rule, there are buttons for 'Add new notification' and 'Cancel'.

McAfee™ Dashboards Governance Analytics Incidents Policy Reports Custom Apps

Cloud Governance ☒ on

Trigger an email notification for changes in Service Risk.

My Notifications

on/off Send an email notification for these Saved Views:

All Active Services IF Risk Values = An Increase in Risk Score & Any Change X

Add new notification

Cancel

= An Increase in Risk Score & Any Change

台帳未掲載のサービスを見つける

➤ 標準機能もあるが、UTMのログのほうが早い

 [Dashboards](#) [Governance](#) [Analytics](#) [Incidents](#) [Policy](#) [Reports](#) [Custom Apps](#)  

Unmatched Uploads

Unmatched Uploads include any outbound traffic events to services that are not identified by our Global Registry. Sort and search by URL to determine how much data your users are passing to these services. This information can be exported in a CSV file.

UNMATCHED UPLOADS



 CSV

URL	UPLOAD COUNT ▼	UPLOAD DATA	USERS	NO OF DAYS
http://www.google.com	8.4 M	219.1 GB	27.8 K	422
http://www.facebook.com	7.1 M	164.3 GB	81.5 K	454
http://www.youtube.com	5.1 M	118.1 GB	29.7 K	453
http://www.linkedin.com	4.8 M	371 GB	9,367	184
http://www.instagram.com	4.8 M	393.9 GB	9,397	185
http://www.twitter.com	4.3 M	101.3 GB	24.3 K	453

例) PAN社のData Filtering機能

➤ ファイルの持ち出しをIDPSログに記録し、相関分析

☐	Name	Location	Rule Name	Applications	File Types	Direction	Action
☐	basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, torrent, vbe, wsf	both	block
					File Types	Direction	Action
					encrypted-rar, encrypted-zip	both	continue
					any	both	alert

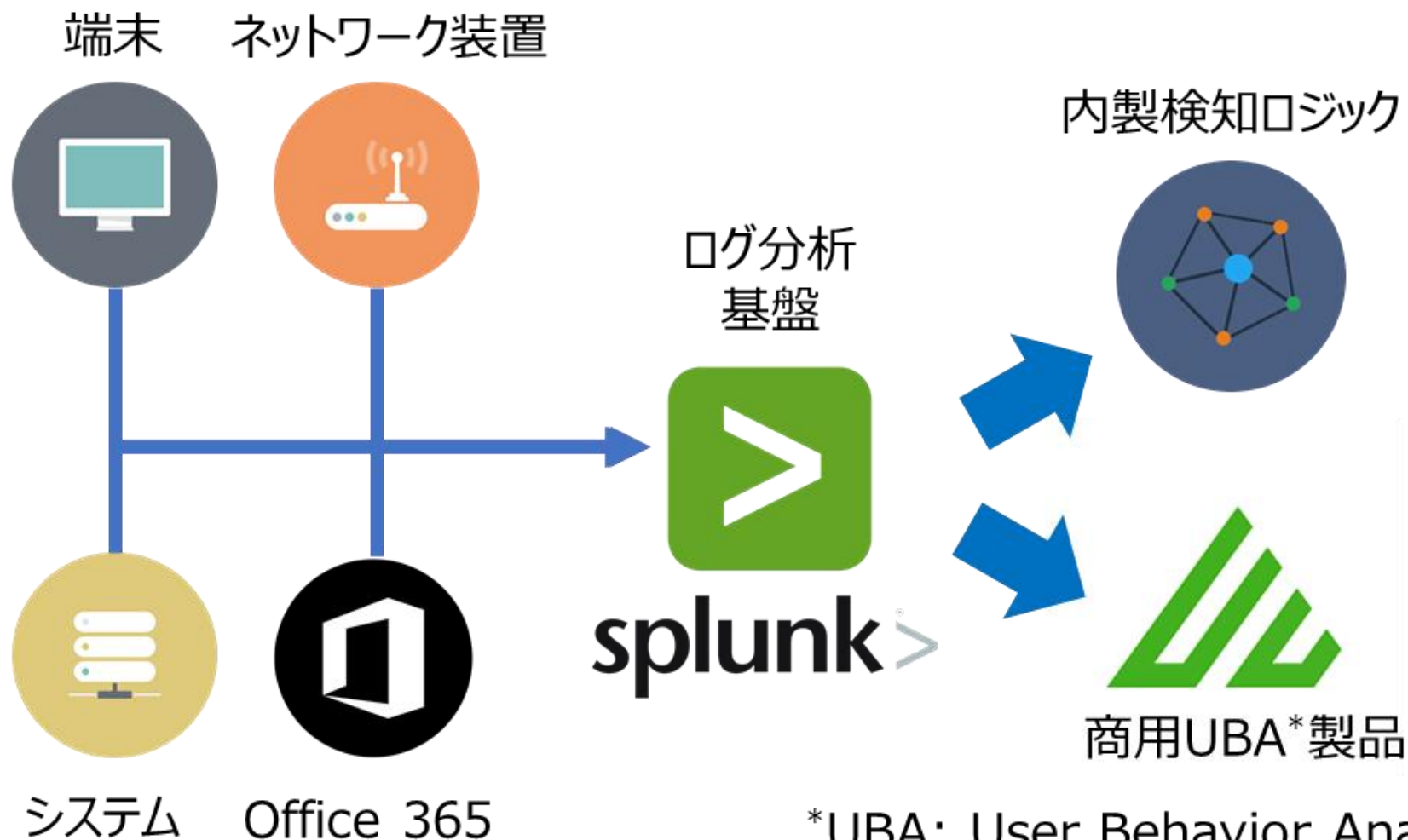
Create Best Practice Security Profiles for the Internet Gateway

<https://docs.paloaltonetworks.com/best-practices/9-0/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/create-best-practice-security-profiles>

利用開始後の運用（再掲）

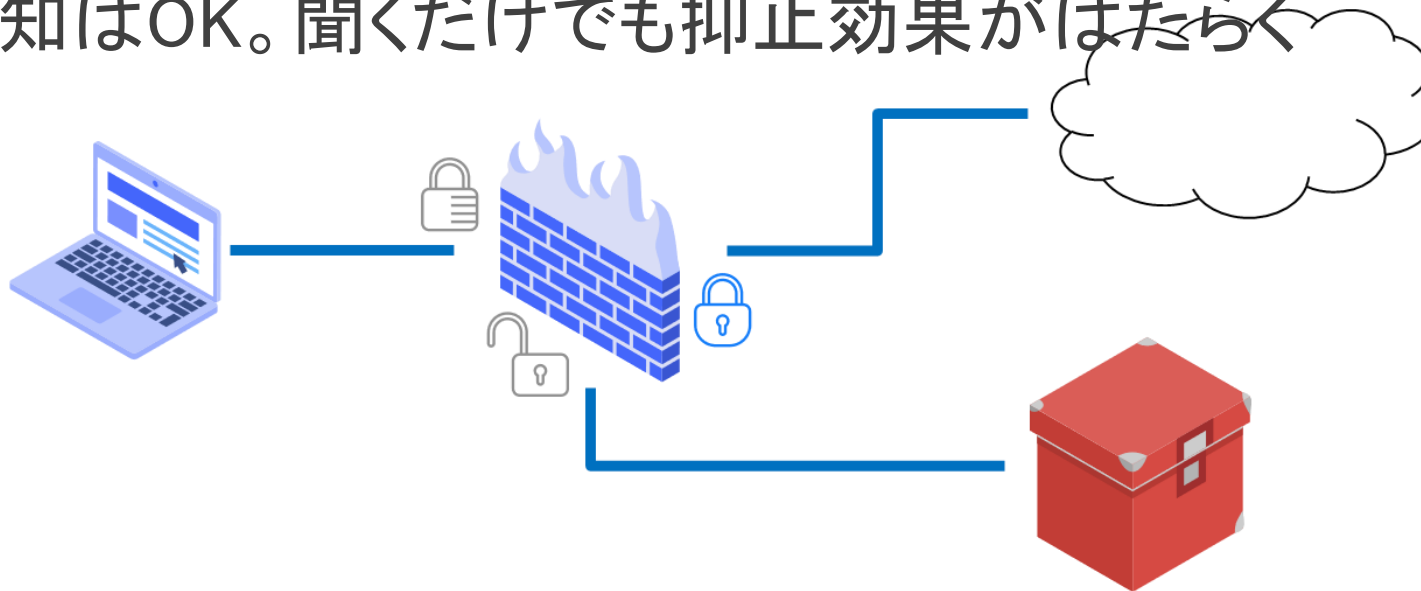
	①サービス事故	②不適切使用
事前規制	格付に基づく選別	ID連携の強制
事後チェック	格付変化の追跡	未届け利用の発見 アップロードの監視

当社の内部不正監視



アップロードファイルを監視する

- SSL/TLSを復号し、パケットを取得する
- ファイルを検査し、不審なら本人 and/or 上司に聞く
- 誤検知はOK。聞くだけでも抑止効果がはたらく



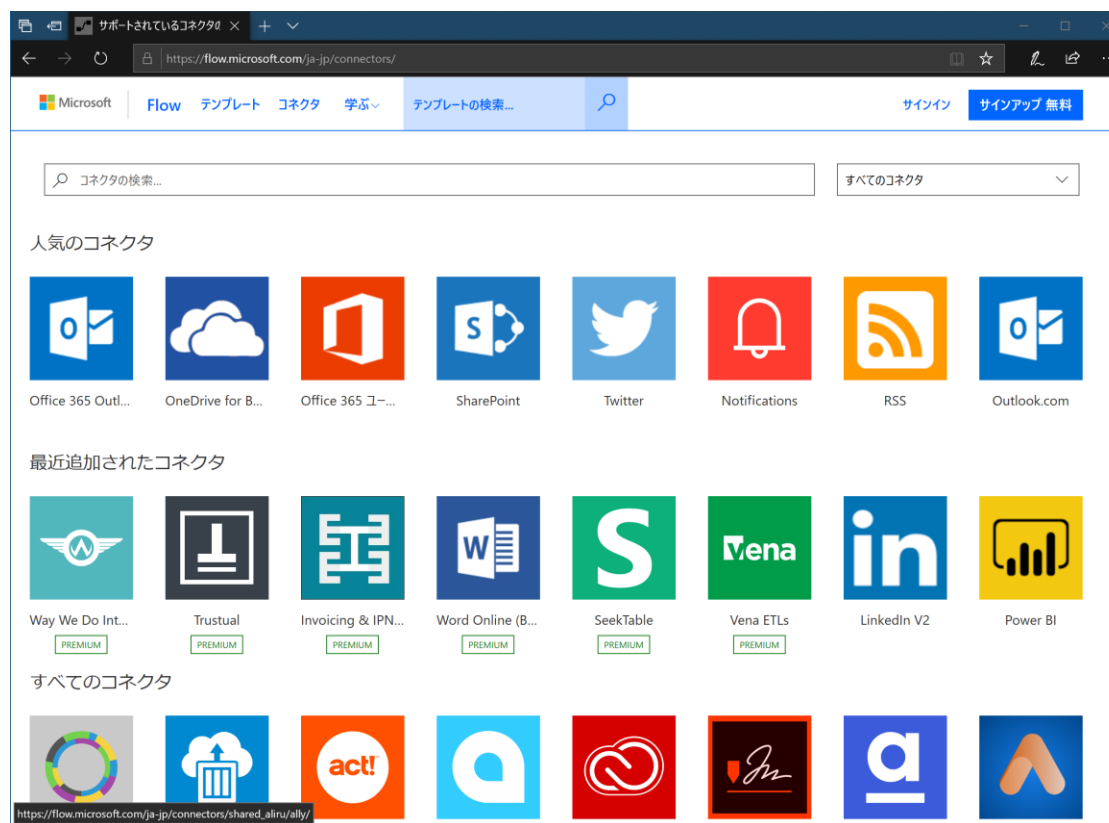
ネットワークフォレンジック装置



課題と展望

技術的課題: Office 365

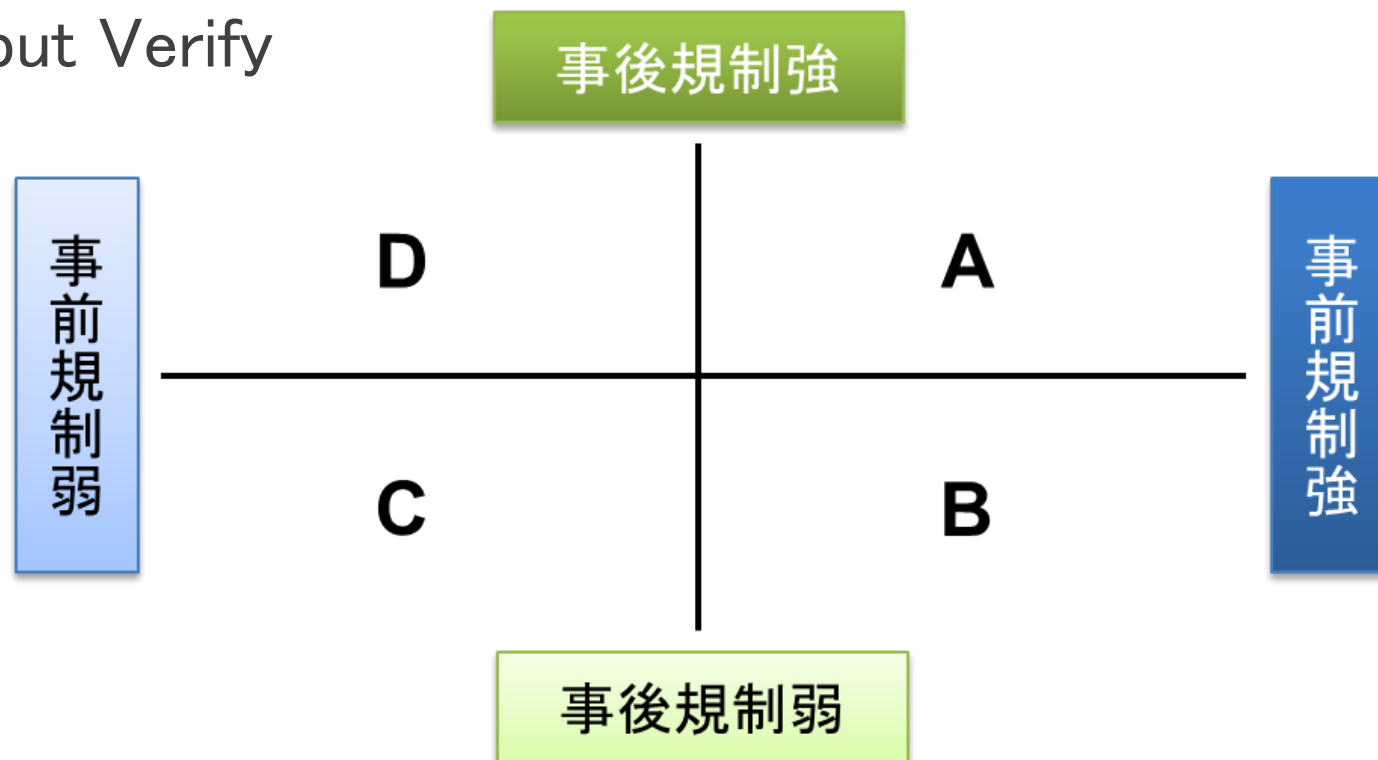
- 企業内ネットワークを通過せずにデータの授受ができる
- より高価なオプションを買うしかないのか？



組織的課題：事前審査の簡素化

➤ 規制改革の理念は、事前規制から事後チェックへの移行

➤ Trust but Verify



内閣府 総合規制改革会議「中間とりまとめ」(2002年)

<https://www8.cao.go.jp/kisei/siryo/>

参考)タイプBの得失

	メリット	デメリット
タイプB	● 事前規制があるので行動規範を示し得る ● 事後規制をあまりしないので運用コストが大きくなり過ぎない	● 規制が尻抜けになる ● 事後規制が弱いのでルールの裏をかく者が続出し正直者が馬鹿を見ると皆がルールを建前視してしまう ● ルールの建前化を防止しようとインフォーマルな手法(行政指導等)に頼るとルール運営が不透明になる ● 事前規制の存在が関係者の創意工夫を削ぎかねない

事前規制と事後規制の類型化

<https://www8.cao.go.jp/kisei/siryo/020723/4-b.pdf>

おわりに

- ▶ クラウドサービスを安全に使ってもらうには、事前規制と事後チェックとを組み合わせた仕組みづくりが大切です
- ▶ CASBをインテリジェンスとして活用することが非常に有効！
- ▶ 日本のユーザー企業も、サービス事業への要求を通じて日本のセキュリティの向上に寄与できます
- ▶ ご関心のある方は、ぜひCASB WGにご参加ください

ご清聴ありがとうございました

CSAジャパンの活動の最新状況については、以下を参照ください
<http://cloudsecurityalliance.jp>

