



クラウドの安全利用を促進するための CASBを用いた業務設計と運用

2019年11月7日

渡辺 慎太郎／サイバーセキュリティ推進部

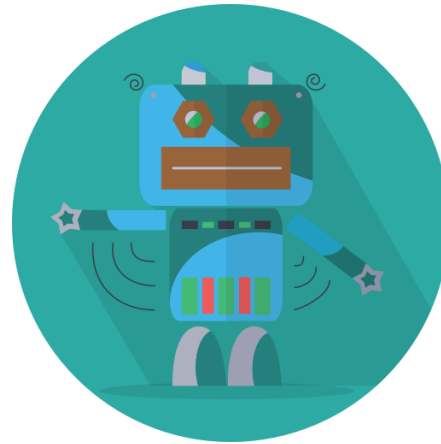
CISA, CISSP, GCIH, GCFA, 産業技術大学院大学認定登録講師

株式会社ジュピターテレコム

DX



DevOps



RPA



SaaS

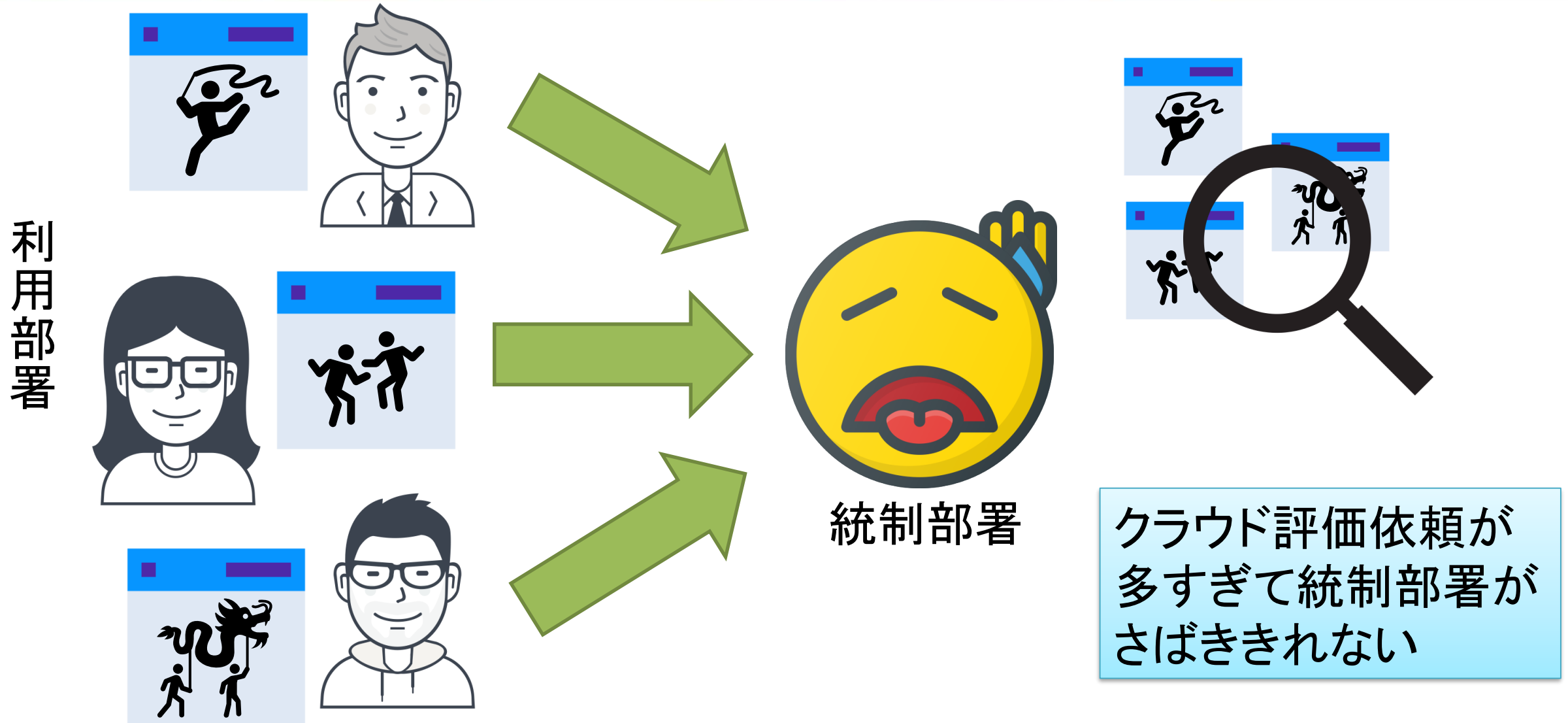
ちよいデジ 協同組合



クラウド統制の不幸なケース①

もっと、あなたに響くこと。

J:COM

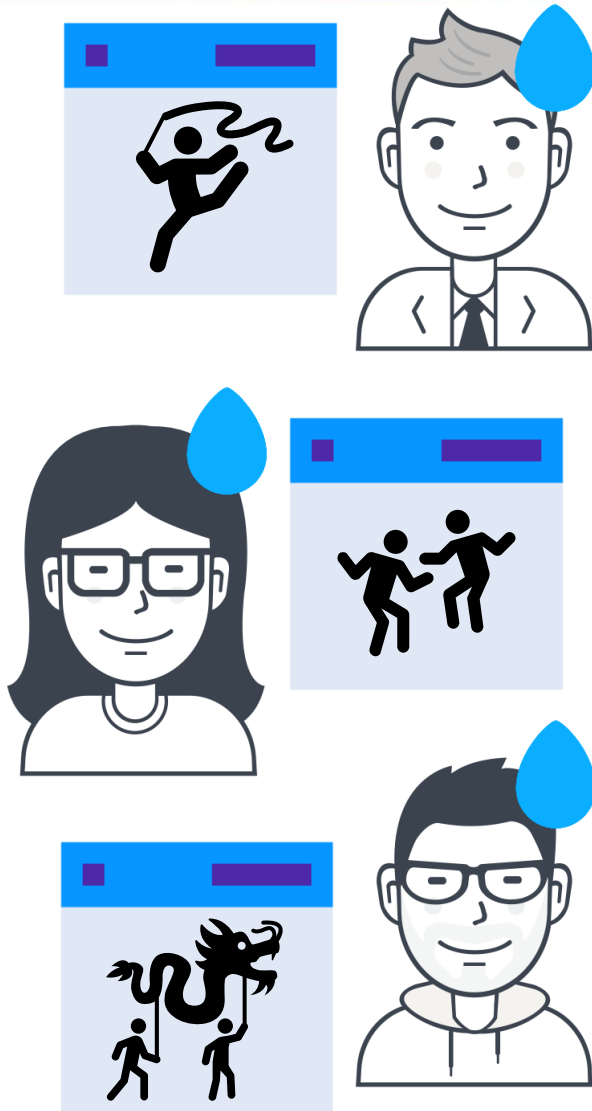


クラウド統制の不幸なケース②

もっと、あなたに響くこと。

J:COM

利用部署



統制部署

自分で
調べてね

統制部署が
クラウド評価を
現場に丸投げする

疲労度 DX

- 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
 - 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

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

クラウドの脅威源はどこにあるか？

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://www.itmedia.co.jp/enterprise/articles/1901/28/news084.html>

- 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）

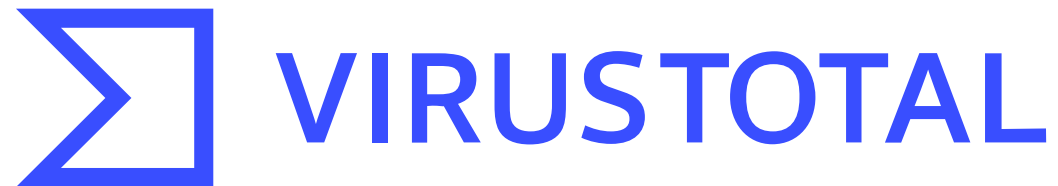
<https://internet.watch.impress.co.jp/docs/news/1185500.html>

クラウドの脅威源はどこにあるか？

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の使い方注意

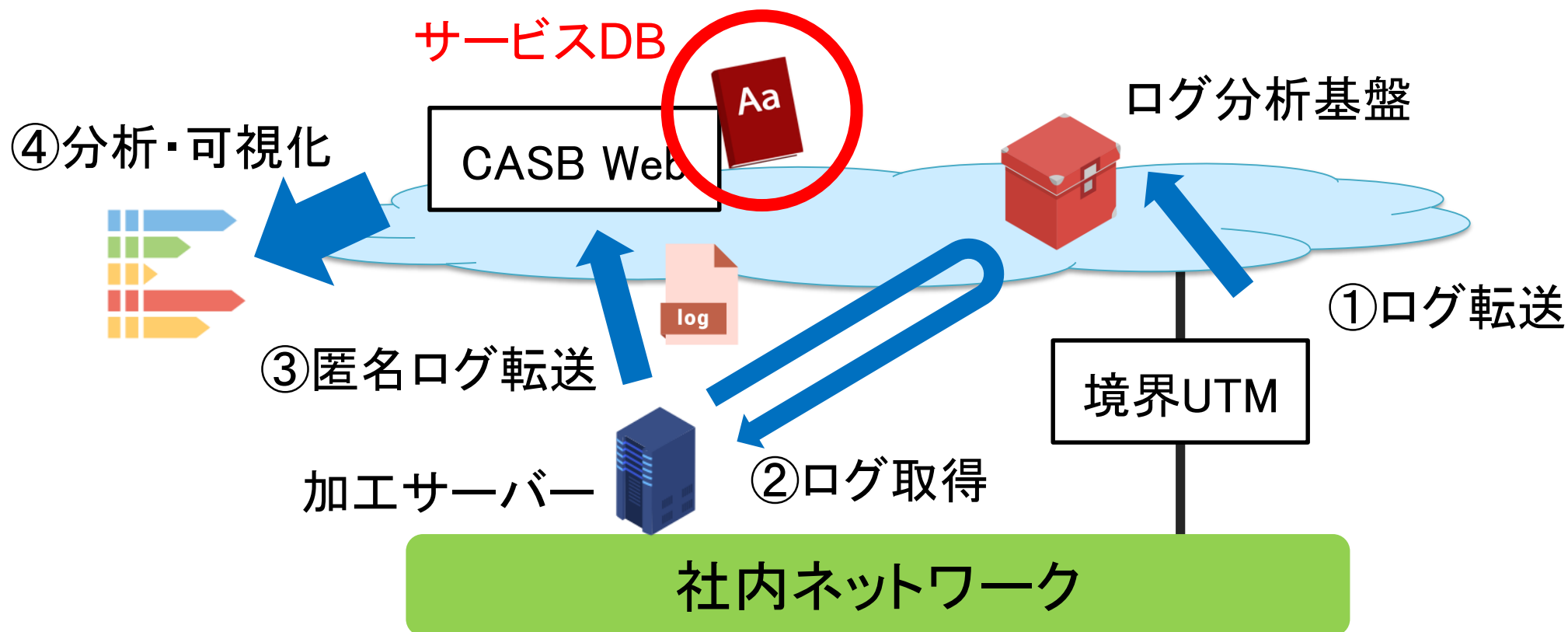
<https://www.itmedia.co.jp/enterprise/articles/1603/14/news104.html>

● クラウドの脅威に対する対策の例

	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

● 我々にとってのCASB: サービス格付機関 兼 利用状況可視化ツール



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

<input type="checkbox"/>	Name	Public ↓	Users	Public	Users	Outbound Data	Inbound Data	Users	Access Count
<input type="checkbox"/>	samurai-olga-media	✓		✓		8 MB	321 MB	197	361
<input type="checkbox"/>	lavo-images	✓		✓		8.8 MB	339 MB	107	598
<input type="checkbox"/>	ul-erw-production	✓		✓		18.2 MB	305.6 MB	728	3,840

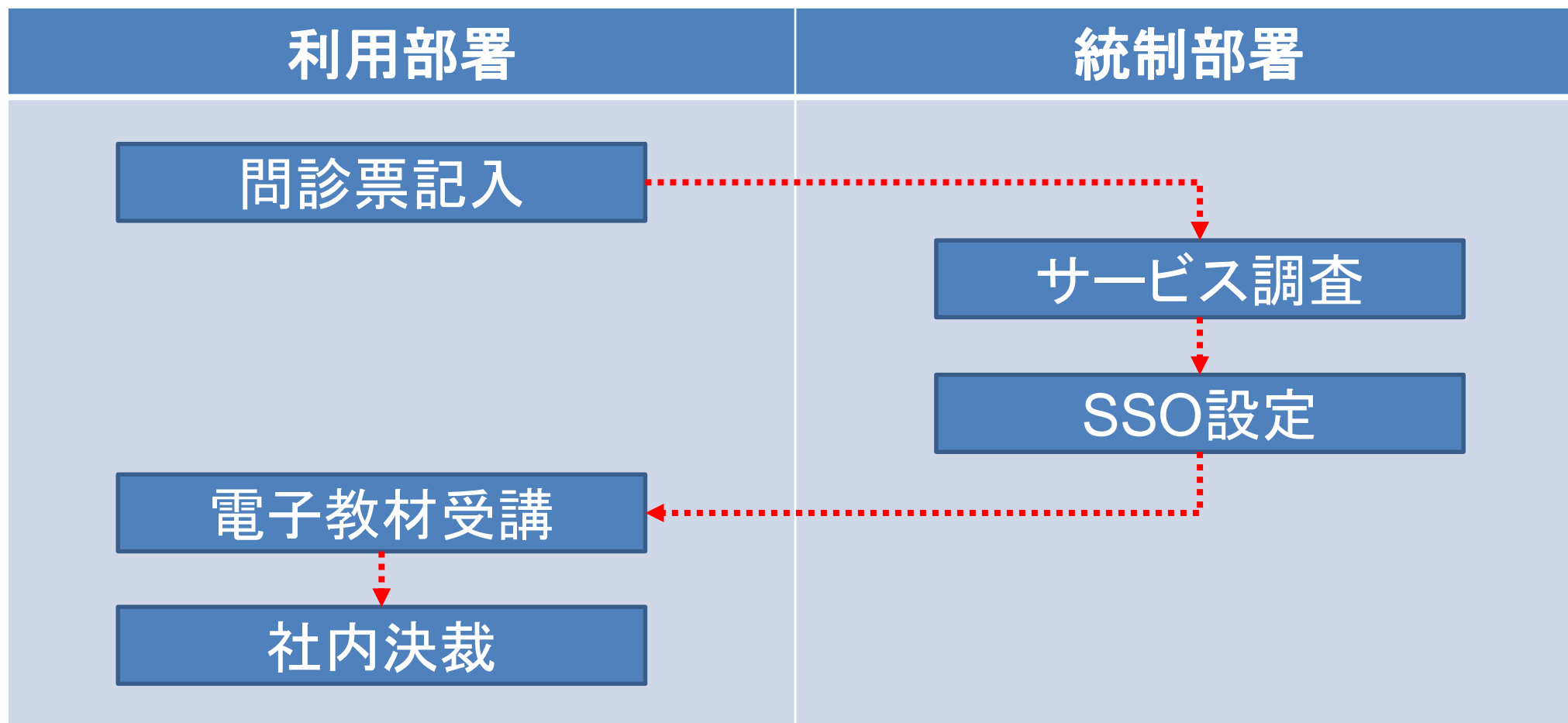
● クラウドの脅威に対する対策の例

	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)

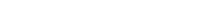
もっと、あなたに響くこと。

J:COM





問診票記入 → 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乗せる
 - Excelはやめましょう



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

Cloud Registry >

Sansan

Approved

Actions

Overview

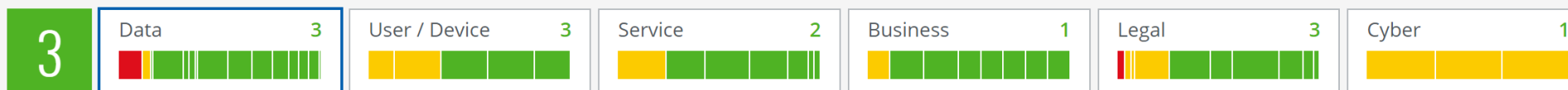
Risk

Usage

Traffic

Risk Score Last updated Apr 23, 2019 UTC

■ High Risk ■ Medium Risk ■ Low Risk



Data Risk: 3

	Category	Attribute	Value	↓ Score	Attribute Weight	Weighted Score	Review Date	Notes
>	<div><div></div></div>	Data Sharing	File Sharing Support	<div><div></div></div> Yes 80	12%	30	Apr 2019	+
>	<div><div></div></div>	Data Loss Protection	Integrated Data Loss Prevention Controls	<div><div></div></div> No 60	4%	10	Apr 2019	+
>	<div><div></div></div>	Encryption	Signature Algorithm of SSL Certificate	<div><div></div></div> SHA256 With RSA Encryption 30	1%	1	Apr 2019	+
>	<div><div></div></div>	Data Retention	Data Retention Policy Upon Account Deletion	<div><div></div></div> 15 to 30 days 20	15%	11	Apr 2019	+
>	<div><div></div></div>	Encryption	Data Encryption in Transit	<div><div></div></div> TLS 1.0 20	3%	2	Apr 2019	+
			<div><div></div></div> TLS 1.1 10	10%	1			

● McAfeeの資源を活用する

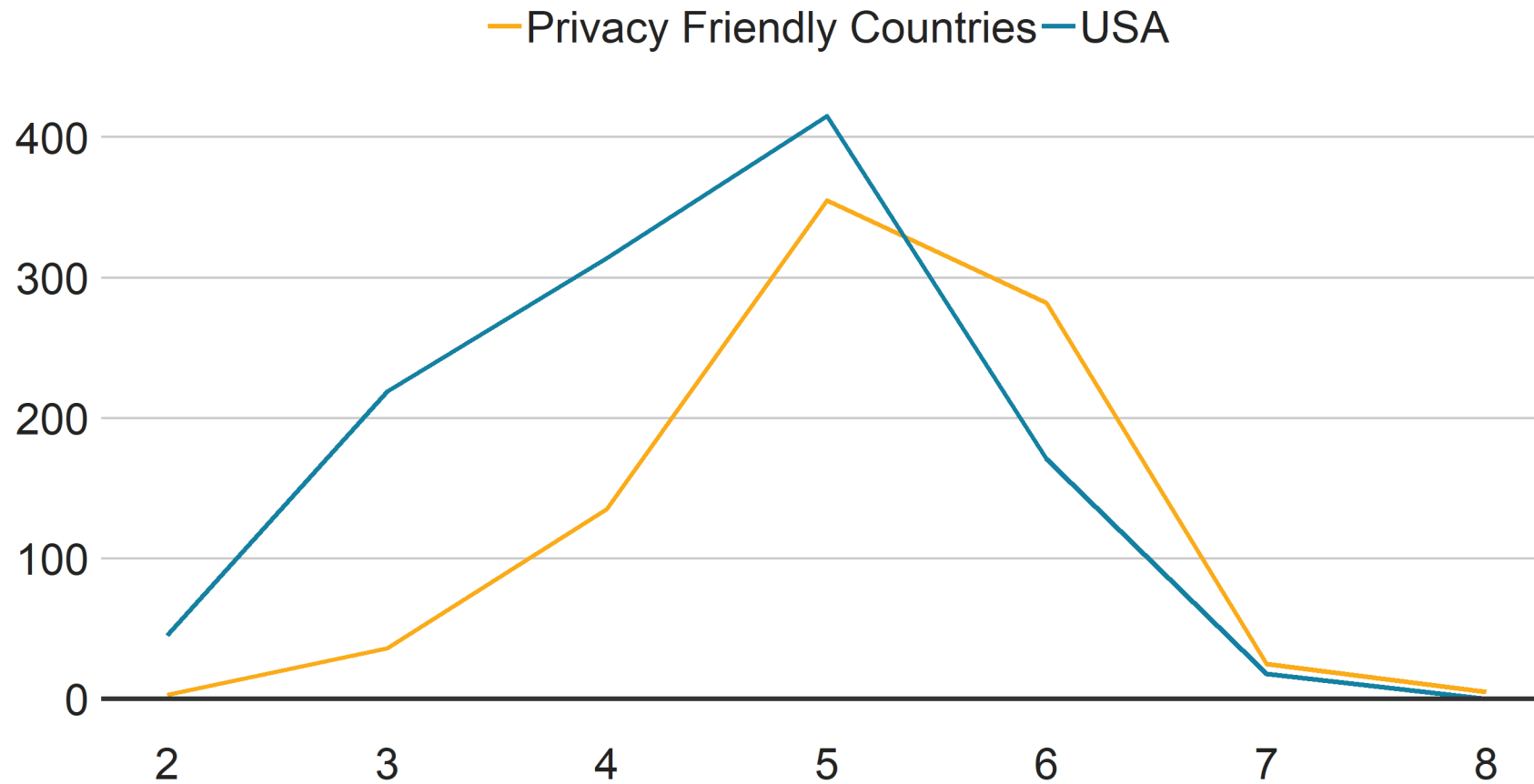
- 台帳に載っていないサービスは即座にリクエスト
 - MVISION Cloudの長所は、応答が迅速な点(だった)

● McAfeeの権威を活用する

- リスク値の悪いもの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

Risk Score Distributions

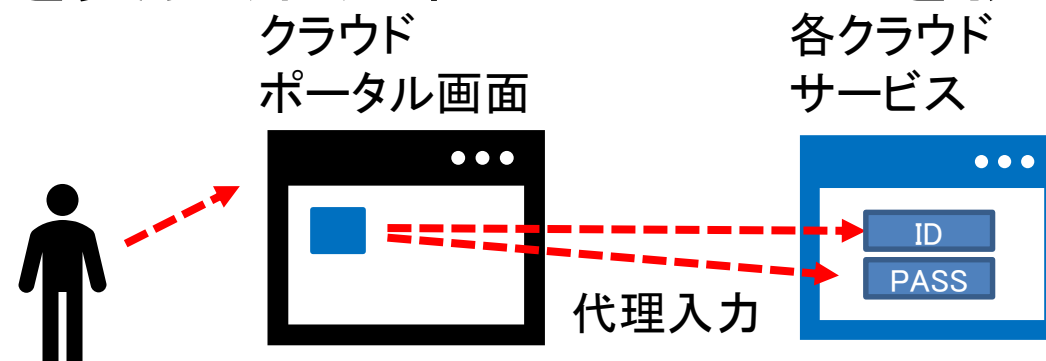
grouped by the location of Business HQ



● 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



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

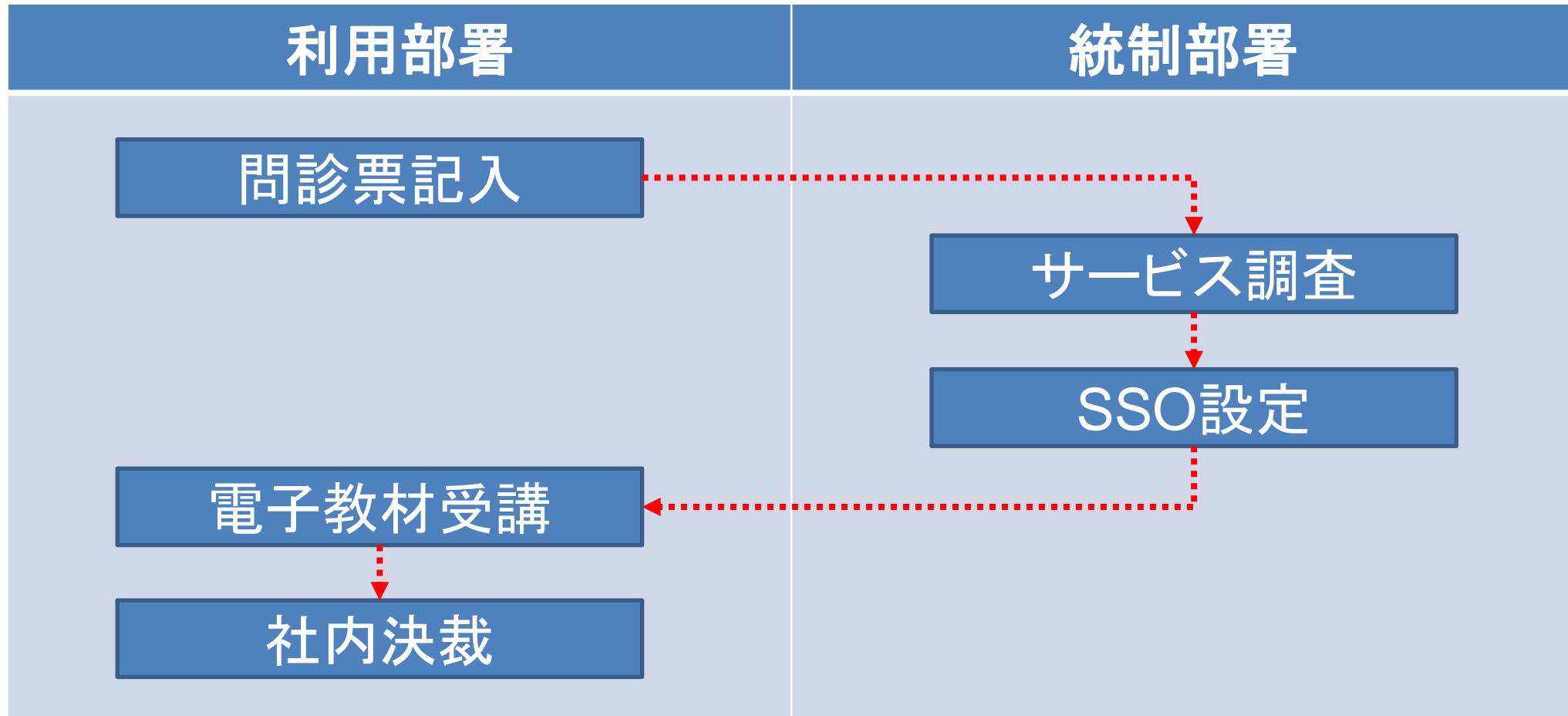
ページ数: 18ページ

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)

もっと、あなたに響くこと。

J:COM

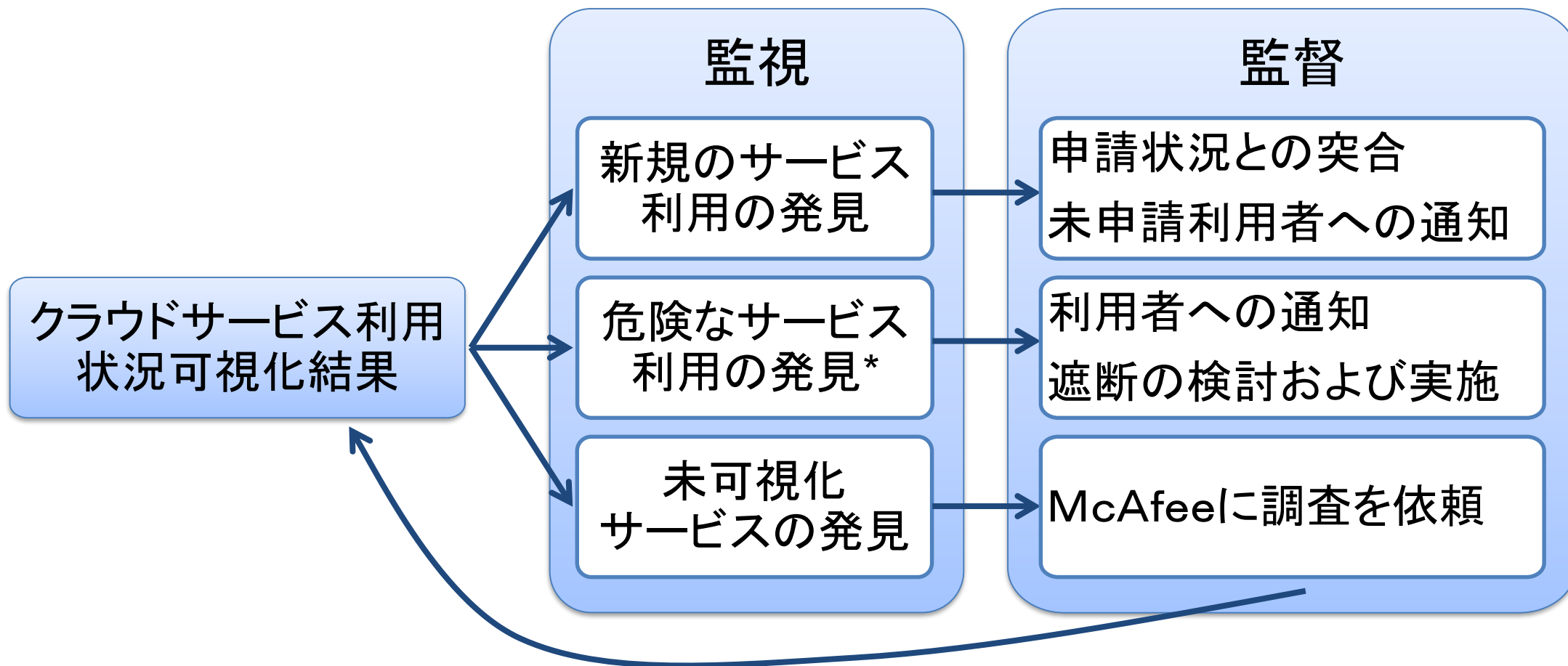


ルールを作り、説明する

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

	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



* 利用中に危殆化する場合も含む



Dashboards

Governance

Analytics

Incidents

Policy

Reports

Custom Apps



My Dashboard

Actions



New Services

37 +18 (95%)

48 Users | 860 KB Upload Data



Last 7 Days

Unassigned Services

34 0 (0%)

2 Low | 32 Med | 0 High



High Risk Services

35 +6 (21%)

27 Allowed | 2 Denied | 6 Partially Allowed



Last 7 Days



Users with Uploads greater t...



6 Partially Allowed

リスク値が変化したときに通知させる

もっと、あなたに響くこと。

J:COM

The screenshot shows the McAfee Cloud Governance interface. The top navigation bar includes the McAfee logo and links to Dashboards, Governance, Analytics, Incidents, Policy, Reports, and Custom Apps. The main content area is titled "Cloud Governance" and has a toggle switch set to "on". Below this, it says "Trigger an email notification for changes in Service Risk." and "My Notifications". Under "My Notifications", there is a section "on/off Send an email notification for these Saved Views:". A notification rule is configured with a bell icon, "All Active Services", "IF Risk Values", and "= An Increase in Risk Score & Any Change". A callout box highlights the condition "= An Increase in Risk Score & Any Change". Another callout box highlights the "Add new notification" button. A "Cancel" button is also visible.

Settings

myshn.net/setup-and-configuration/#/user-notification

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


Add new notification

Cancel

= An Increase in Risk Score & Any Change

台帳に載っていないサービスを見つける

● 標準機能もあるが、UTMのログを見たほうが早い

 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.example.com	8.4 M	219.1 GB	27.8 K	422
http://www.example.com	7.1 M	164.3 GB	81.5 K	454
http://www.example.com	5.1 M	118.1 GB	29.7 K	453
http://www.example.com	4.8 M	371 GB	9,367	184
http://www.example.com	4.8 M	393.9 GB	9,397	185
http://www.example.com	4.3 M	101.3 GB	24.3 K	453

● ファイルの持ち出しをIDPSのログに記録させ、相関分析する

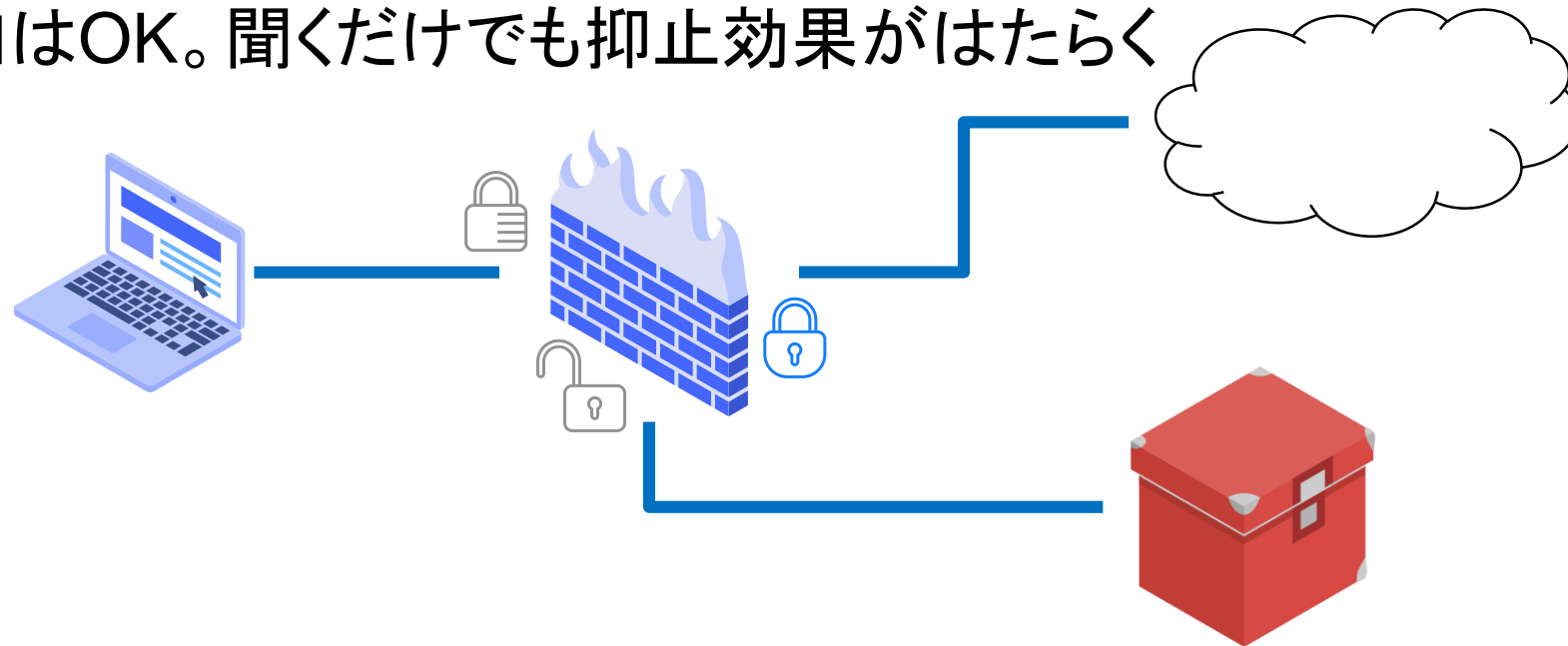
<input type="checkbox"/>	Name	Location	Rule Name	Applications	File Types	Direction	Action
<input type="checkbox"/>	basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, torrent, vbe, wsf	both	block
					rypted-rar, rypted-zip	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>

	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

- 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

どうやって効率化するか？

もっと、あなたに響くこと。

J:COM

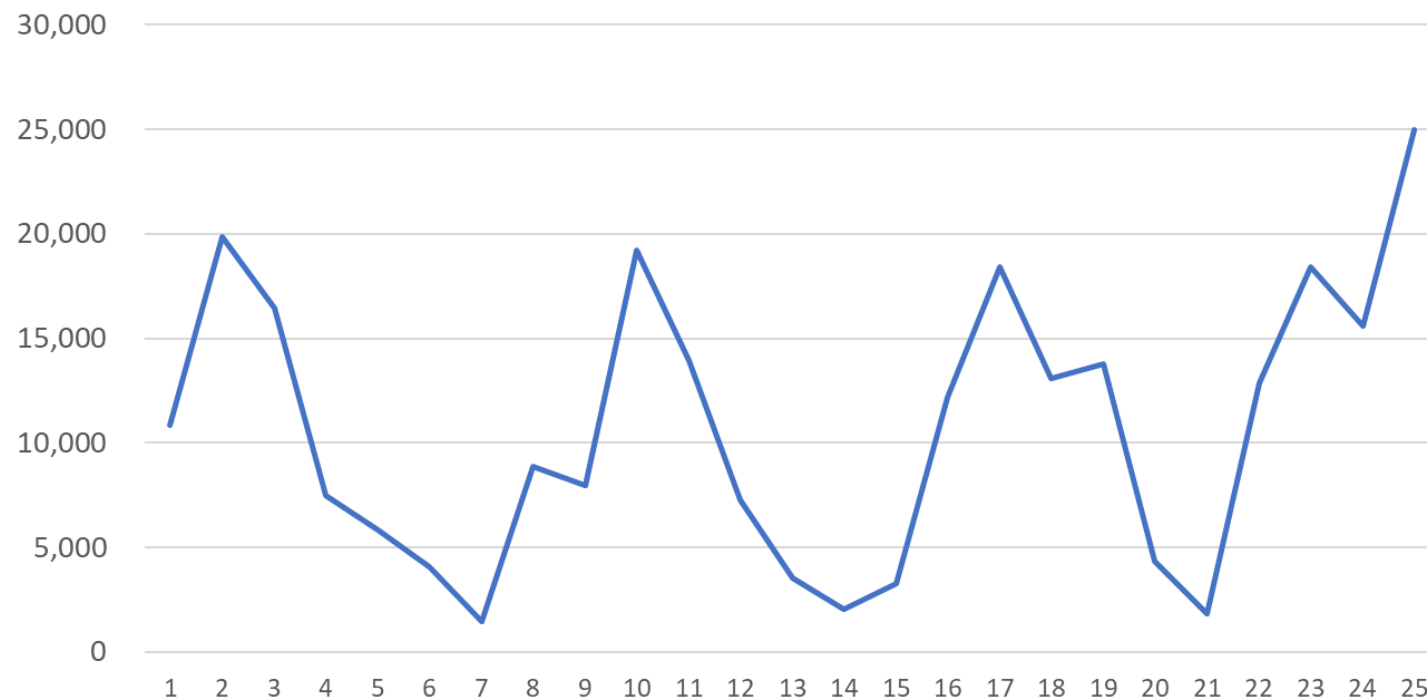
● 検査対象を減らす

➤ 方法1 カテゴリーによるブロック

- Online Storage
- Webmail など



過剰ブロックの発生



● 検査対象を減らす

➤ 方法2 HTTPヘッダーを見る

アップロードに関するHTTPリクエストヘッダーの例

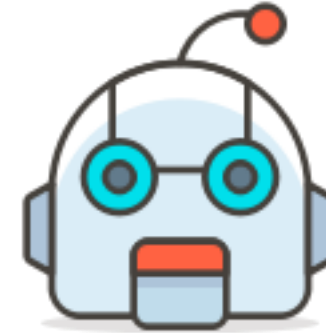
- Content-Length
- Content-Range
- Transfer-Encoding (ここにはサイズがない)



どうやって効率化するか？

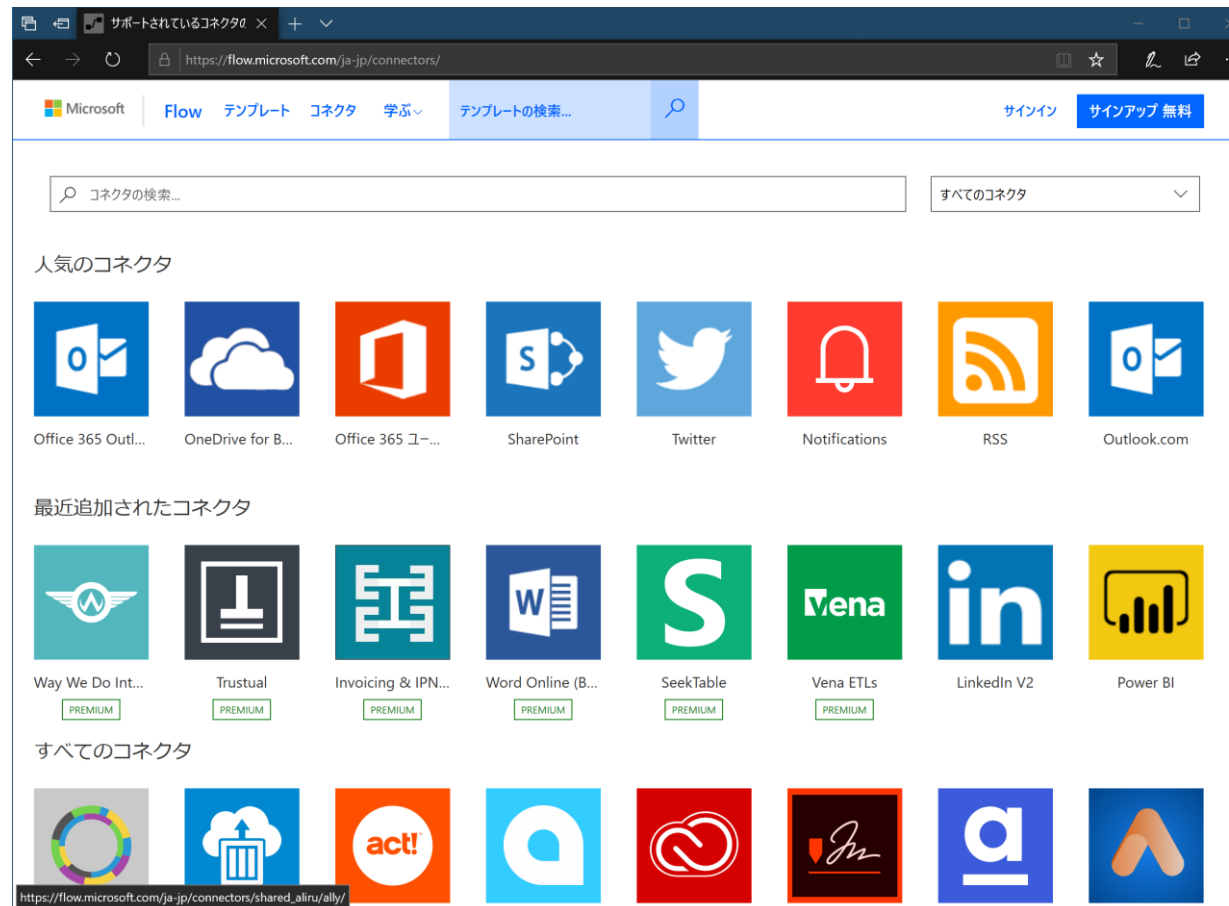
● 検査を自動化する

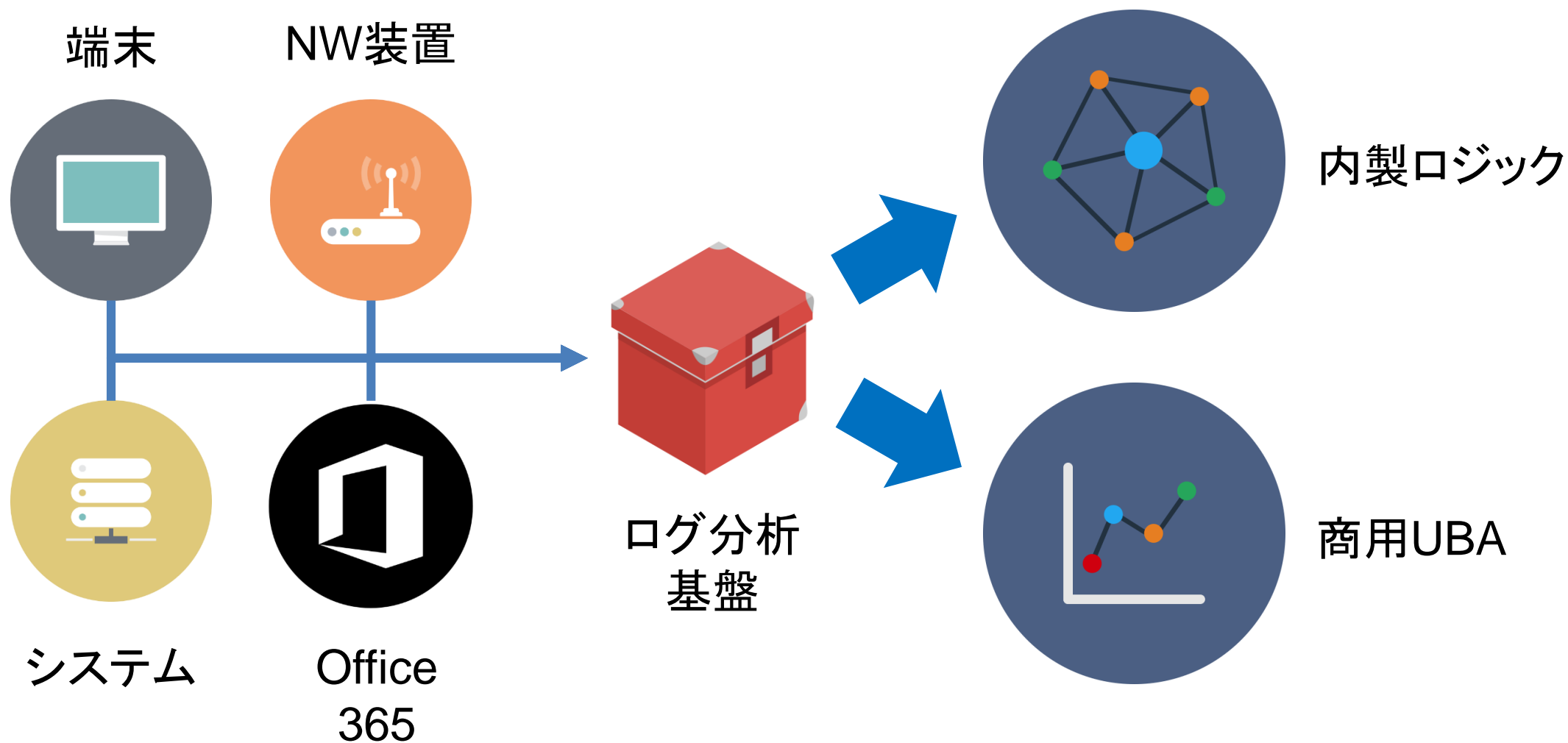
- ファイルの中身を検査するツールは複数存在
 - ・ クレカやマイナンバーなどは容易
 - ・ 個人情報とは？
- 方法1 セグメントを分離する
 - ・ 別セグメントにアップロード専用ブラウザを用意し、ファイルを別セグメントのサーバーにコピーする
- 方法2 ネットワークフォレンジック装置を使う
 - ・ パケットからファイルを自動抽出する



課題① Office 365の進歩についていけるか？

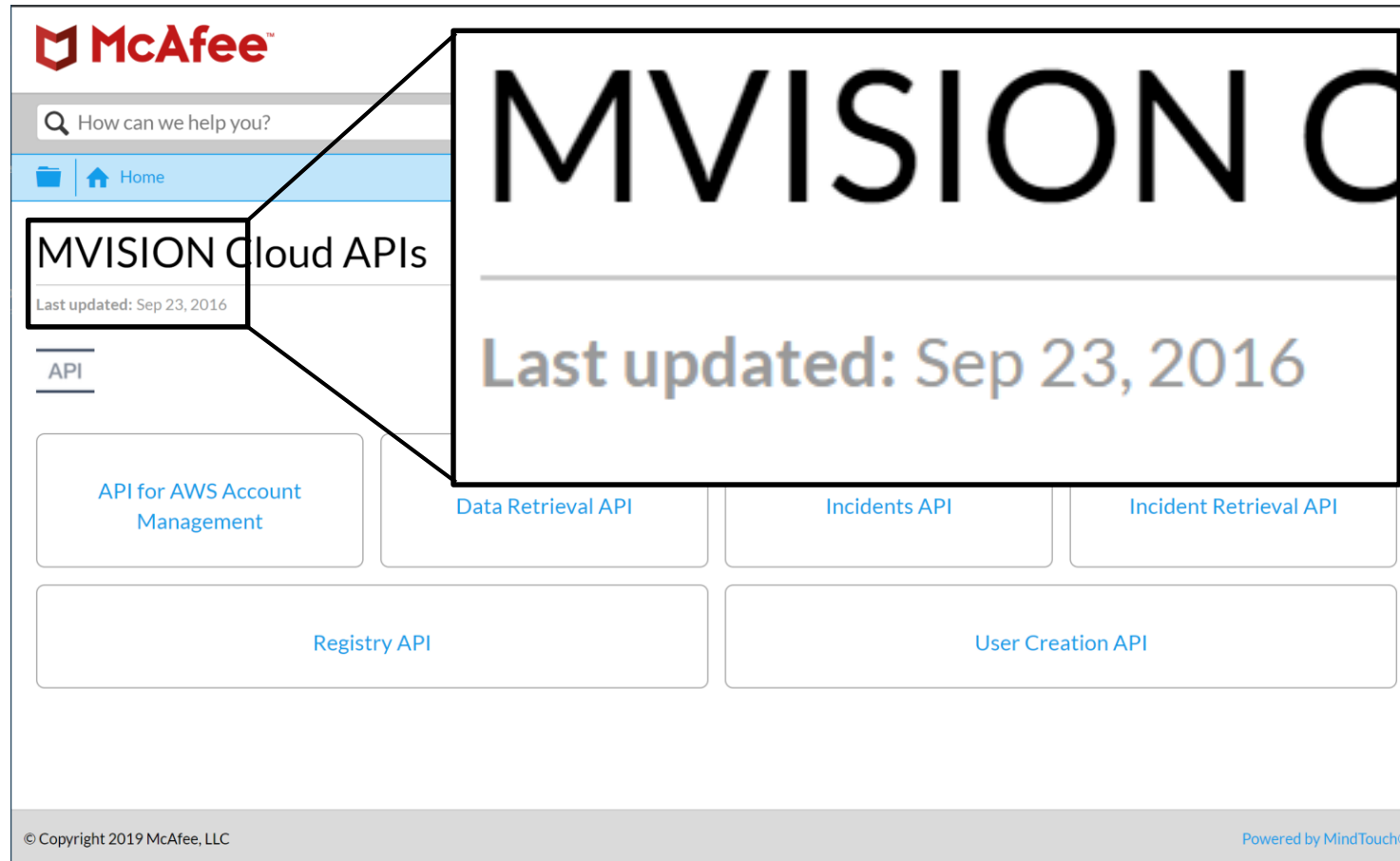
- 企業内ネットワークを通過せずデータの授受ができる
 - ダッシュボードで見られる内容が必ずしもログで取得できない



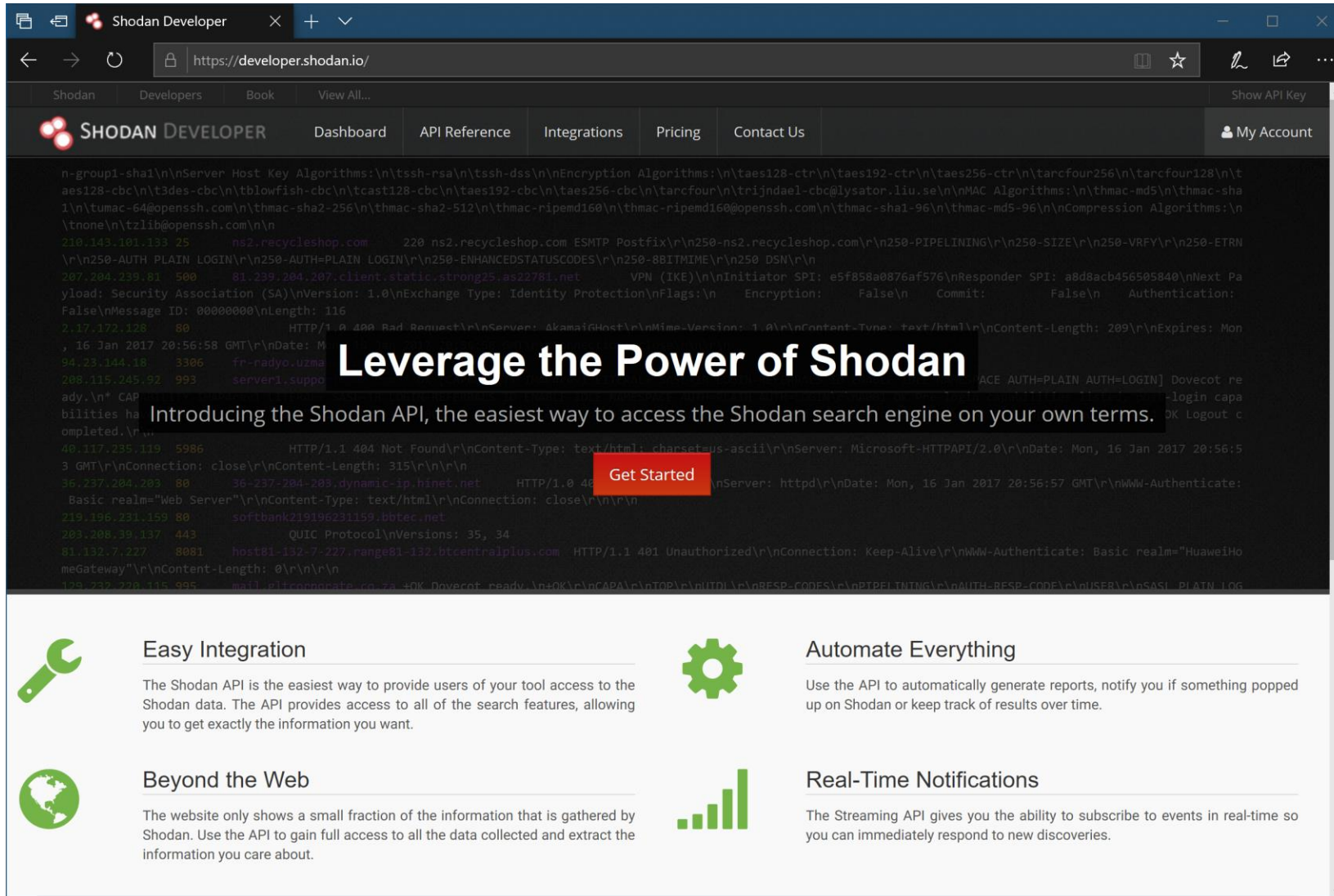


課題② もっと自動化できないか？

- CLIで操作したい
 - 取得系はあるのだが、更新系がない







参考)APIに優れる情報提供サービスの例



Leverage the Power of Shodan

Introducing the Shodan API, the easiest way to access the Shodan search engine on your own terms.

[Get Started](#)

- 
Easy Integration
 The Shodan API is the easiest way to provide users of your tool access to the Shodan data. The API provides access to all of the search features, allowing you to get exactly the information you want.
- 
Automate Everything
 Use the API to automatically generate reports, notify you if something popped up on Shodan or keep track of results over time.
- 
Beyond the Web
 The website only shows a small fraction of the information that is gathered by Shodan. Use the API to gain full access to all the data collected and extract the information you care about.
- 
Real-Time Notifications
 The Streaming API gives you the ability to subscribe to events in real-time so you can immediately respond to new discoveries.

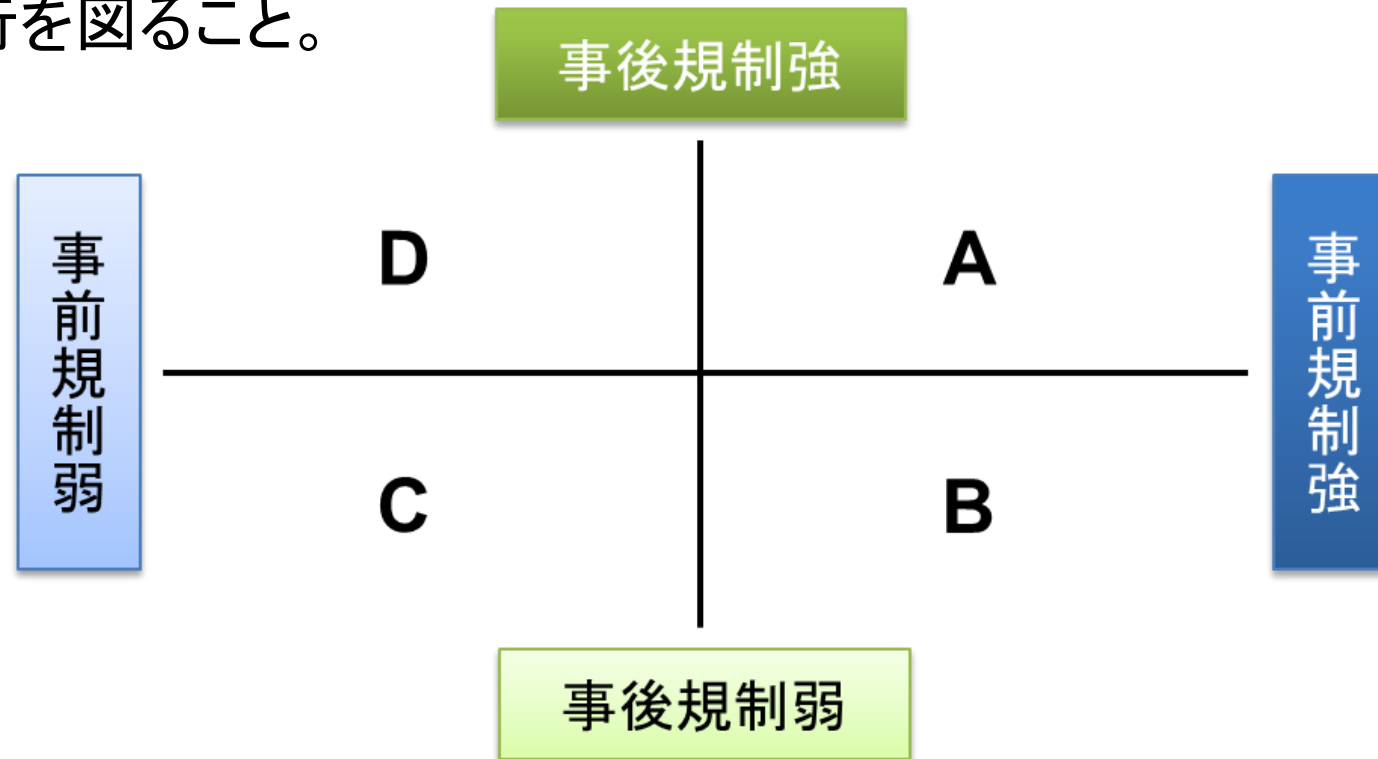
参考) 日本でポート5555番が空いているホストのAS順は？

●R言語による10行サンプル

```
response <- httr::GET("https://api.shodan.io",  
  path = "shodan/host/search",  
  query = list(  
    key = SHODAN_API_KEY,  
    query = "country:JP port:5555",  
    facets = "asn:100"  
  )  
)  
results <- jsonlite::fromJSON(httr::content(response, as = "text"))  
dplyr::as_tibble(results$facets$asn)
```

課題③ 事前審査を簡素化できないか？

- 規制改革の基本理念は、「事前規制」から「事後チェック」(監視・監督)への移行を図ること。



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/>

	メリット	デメリット
タイプB	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● 規制が尻抜けになる● 事後規制が弱いのでルールの中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>

	メリット	デメリット
タイプD	<ul style="list-style-type: none">● 事前規制に要するコストがかからない● 一定の部分を除き規制がないので関係者の創意工夫の余地が大きい● 事後規制ルールが行為規範となる	<ul style="list-style-type: none">● 事後規制に要するコストがしばしば大きい● 事後規制は事前規制ほど徹底できないことが多い● 一罰百戒の効果を上げるため制裁措置を高めると不公平感を生みかねず、また違反者の更生を阻害しかねない● 司法機構の強化の反面として行政機構の弱体化を招きかねない

事前規制と事後規制の類型化

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

- クラウドサービスを安全に使ってもらうためには
事前規制と事後チェックとを上手に組み合わせた
仕組みづくりが大切です
 - CASBをインテリジェンスとして使えば、工数が削減できます
- ユーザー企業も、サービス事業者に対する要求を通じ、
日本のセキュリティの向上に寄与できます
- 我々の取り組みは始まったばかりです。
ぜひみなさんの取り組みもお聞かせください。
WatanabeShint@jupiter.jcom.co.jp