

# インシデントレスポンスを自動化で支援する Slack Bot で人機一体なセキュリティ対策を実現する - SEASON2

伊藤洋也 / GMO PEPABO inc.

2023.03.18 YAPC::KYOTO 2023 Reject Con

GMOペパボ

GMOペパボ セキュリティ対策室

伊藤 洋也

Hiroya Ito

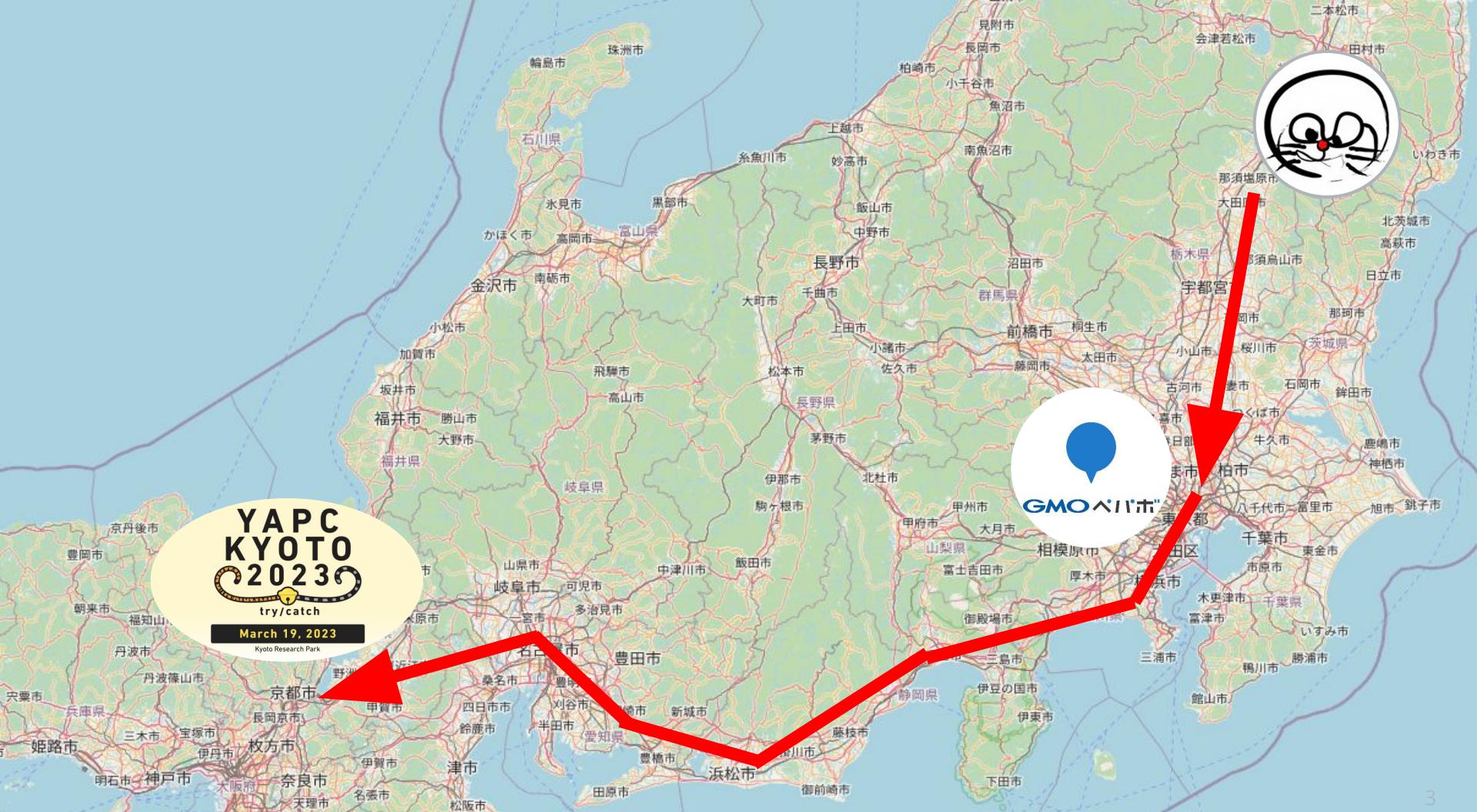
2007年 入社

セキュリティ対策室に所属

組織横断のセキュリティ対策をやっています

- Twitter : @hiboma
- YAPC Asia 2009 に登壇してから 13年ぶり!





JP / EN

サイト内検索



企業情報

ニュース

サービス

株主・投資家情報

サステナビリティ

採用情報

# 人類のアウトプットを増やす

私たちはインターネットやテクノロジーの力で情報発信のハードルを下げ、あらゆるアウトプットを世界中に増やします。  
さまざまなアウトプットが進化や価値を生み出すように、私たちもプロダクトを生み出し続け、ユーザーと共に進化し拡大していきます。

企業情報

IRトピックス

## 「第21期 定時株主総会」のご案内

2023年3月23日(木)11時00分～開催

プレスリリース

IRニュース

グループ会社ニュース

## サービス一覧

国内最大級レンタルサーバー



高速オールSSDレンタルサーバー



ドメイン取得サービス



簡単ホームページ作成サービス



アルバム・写真共有サービス



ネットショップ作成サービス



欲しいものは、作ればいい。



オリジナルグッズ発注サービス



国内最大(※)のハンドメイドマーケット



チーム・教室のための連絡集金サービス



ネットのおサイフ



※ハンドメイド作品の販売を主軸とするハンドメイドマーケット運営会社の公表数値を比較。2021年8月末時点、自社調べ。

明日(3/19)に登壇するGMOペパボの二人を紹介!!



@ryuichi\_1208



@rsym1290

11:55

入門 障害対応 「サービス運用はTry::Catchの繰り返しだよ、ワトン君」 20分

by 渡部 龍一

15:00

4PB(ペタバイト)を超えるオブジェクトストレージをハードウェアからアプリケーションにかけて運用するノウハウ 40分

by 三上 烈史 (みかみ つよし)

1. #インシデントあるある
2. “インシデント” のアウトプット事例
3. GMOペパボのインシデントマネジメント支援ボット
4. 未来の課題

**How** (どうやって作ったか) より **What** (何を作ったか) の話しがメインです

# スライドの注意

## 本スライドでの「インシデント」の定義

GMO ペパボでは インシデント対応マニュアルで インシデントを下記の通り定義します

- 情報資産のうち重要性1、2に属するものについて、アクセス権限がない人が閲覧することができた
  - **(機密性の問題)**
- 情報資産全てを対象にして、なくなってしまった
  - **(完全性の問題)**
- 情報資産全てを対象に改ざんされてしまった
  - **(完全性の問題)**
- 情報資産全てを対象に、一時的に利用できない状態が発生しお客様に影響が発生した
  - **(可用性の問題)**

本スライドに用いるインシデントの記述は、この定義に準じています

# #インシデントあるある

## インシデントの初動、こんなことありませんか？

- どこのチャネルで対応しよう!?
  - 😬 アラート通知が流れるチャネルはどんどんログが流れていく ...
  - 😬 Slack のスレッド(\*) で作業してたら みんな気が付かなかつた ...
- インシデントの対応を始めたけど、人が集まらない!
  - 😬 みんなをチャネルに呼び出すのは気が引ける ....
  - 😬 そもそも、誰を呼び出したらいいんだっけ？

(注) チャネルの会話を枝分かれさせて、一部の人だけで会話を進行する UI

## インシデントの対応中、こんなことありませんか？

- 関係者との連絡がうまくいかない
  - 😬 インシデントが起きたこと、みんなに知らせてないな ....
  - 😬 対応が終わったこと、みんなが知らなかつた ...
- 事前に準備したフローやプロセスが機能しない
  - 😬 どういうフローでやるんだっけ ...? 報告? すぐ対応?
  - 😬 マニュアルを出したけど、みんな無視しちゃうな

## インシデントから復旧後、こんなことありませんか？

- 対応の記録がまとまってない
  - 😐 いつのインシデントだったけ？
  - 😐 どこのチャンネルで対応したっけ？
- 再発防止のアクションが出せない
  - 😐 サマリがなくて 何やったか全体感がわからん
  - 😐 ポストモーテム\* やりたいんだけど 準備が面倒 ...

## みんな 困ってそう?

- ・ みんな、どうやって取り組んでいるのかな?

# “インシデント” のアウトプット事例

## “インシデント” はホットなアウトプットテーマ (\*)

- ・ テックブログで、インシデントや訓練をテーマに発信
- ・ 技術情報誌の特集・書籍の発刊
- ・ カンファレンスの開催
- ・ SaaS

注) 定量的なエビデンスはなく、私がそう思っているだけです! 😬

## CloudNative Inc. BLOG

The screenshot shows a blog post titled "インシデント対応訓練をおこないましたよー" (We conducted an incident response training). The post includes a large image of a hand holding a megaphone pointing at a computer screen displaying a shield icon.

引用: <https://blog.cloudnative.co.jp/13419/>

## mercari engineering

The screenshot shows a blog post titled "メルペイにおけるインシデントマネジメントとナレッジシェア" (Incident Management and Knowledge Sharing at Mercari Pay). It features a banner for the "Merpay Advent Calendar 2022".

引用: <https://engineering.mercari.com/blog/entry/20221220-5040a56d02/>

## モノタロウ Tech Blog

The screenshot shows a blog post titled "Googleでもやっている障害対応訓練の「Wheel of Misfortune」をやってみた。" (I tried the 'Wheel of Misfortune' for incident response training, which Google also does). It includes a small image of two people working on laptops.

引用: <https://tech-blog.monotaro.com/entry/2022/09/06/90000>

2022年以降のエントリを任意で掲載しています。「あの事例が載っていない！」というお声があつたら教えてください

## STORES Product Blog

この記事はSTORES Advent Calendar 2022の13日の記事です。

STORES 予約のSREをしている@aa4easyです。少し前にSTORES 予約のチーム内で障害対応のやり方みたいなところの改善を行なったので、どういった課題があって、どういった改善を行なったのかについてご紹介できたらと思っております。

**きっかけと課題**

ある障害が発生した際に障害対応のやり方に関して、チーム内からどのような課題が出てきました。

データアドミネストラ STORES Product Blog 2022

引用: <https://product.st.inc/entry/2022/12/13/090317>

## RAKUS Developer Blog

【ラクス】インフラ運用チームが障害対応時間削減に向けて取り組んだこと

2022/02/18

カジュアルに面接しませんか？

ラクスの技術 / デザイン情報はこちちら

引用: <https://tech-blog.rakus.co.jp/entry/20220218/troubleshooting>

## Ubie テックブログ

インシデントレスポンスを支えるincident.io

Ubie Discovery SREをしているitkqです。Ubie Discoveryでは、incident.ioを2021年10月頃から導入し、Slackを中心としたインシデントレスポンスを行なっています。incident.ioの特徴と、Ubieでの導入から具体的な活用方法を説明します。

Ubie Engineers & Designers Advent Calendar 2022 8日の記事です。

引用: [https://zenn.dev/p/ubie\\_dev](https://zenn.dev/p/ubie_dev)

 Sreake JP / EN

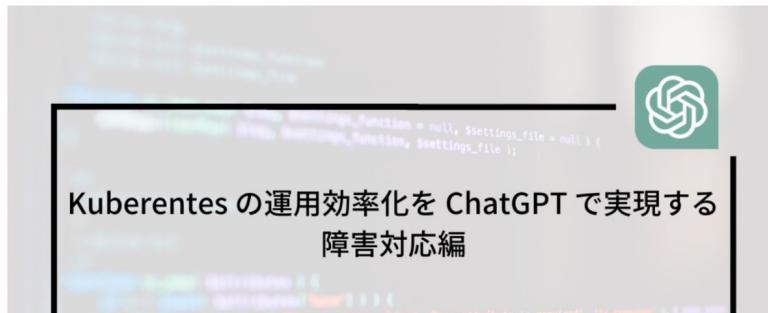
トップ サービス紹介 活用事例 ブログ ホワイトペーパー お問い合わせ

[HOME](#) > [ブログ](#) > Kubernetes の運用効率化を ChatGPT で実現する 障害対応編

# Kubernetes の運用効率化を ChatGPT で実現する 障害対応編

Sreake事業部  
2023.3.16



## Kubernetes の運用効率化を ChatGPT で実現する 障害対応編

**人気記事**

- 1st**  SREとはなにか [サイトリライアビリティエンジニアリング]  
2021.10.25
- 2nd**  SREとインフラエンジニアの違いを3つのポイントで理解する  
2021.8.25
- 3rd**  謎のペールに包まれたGoogleの次世代SIEM「Chronicle」を触ってみた  
2021.6.18
- 4th**  インシデント管理ツール「PagerDuty」とはなにか [特徴・機能・メリット]  
2021.10.1
- 5th**  Datadogのログ管理コストをフィルター機能で削減をする  
2022.6.28

## SoftwareDesign 2022年5月



引用: <https://gihyo.jp/magazine/SD/archive/2022/202205>

## WEB+DB PRESS vol. 119



引用: <https://gihyo.jp/magazine/wdpress/archive/2020/vol119>

## システム障害対応の教科書



引用: <https://gihyo.jp/book/2020/978-4-297-11265-3>

## LEARNING FROM INCIDENTS

LFI

Blog ▾ Podcast Jobs About LFI Conf 2023 Contact Newsletter

### Learning from Incidents in Software

We're a community challenging conventional views and reshaping how the software industry thinks about incidents, software reliability, and the critical role people play in keeping their systems running.

Learn More

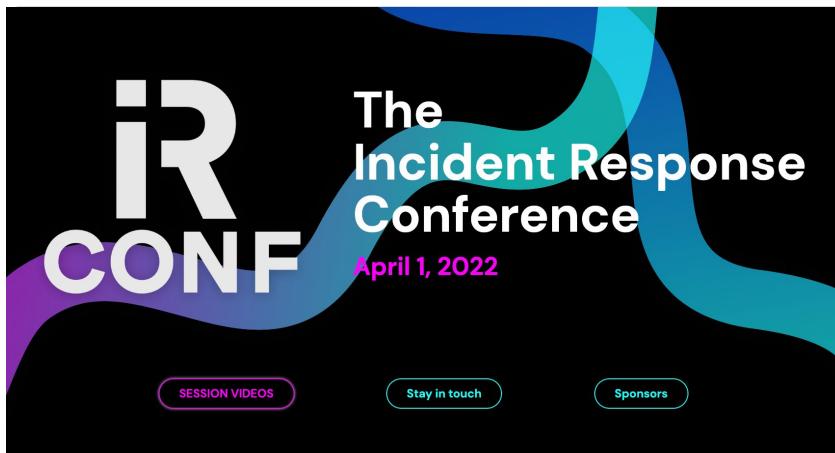


AS SEEN IN FORBES MAGAZINE

Forbes

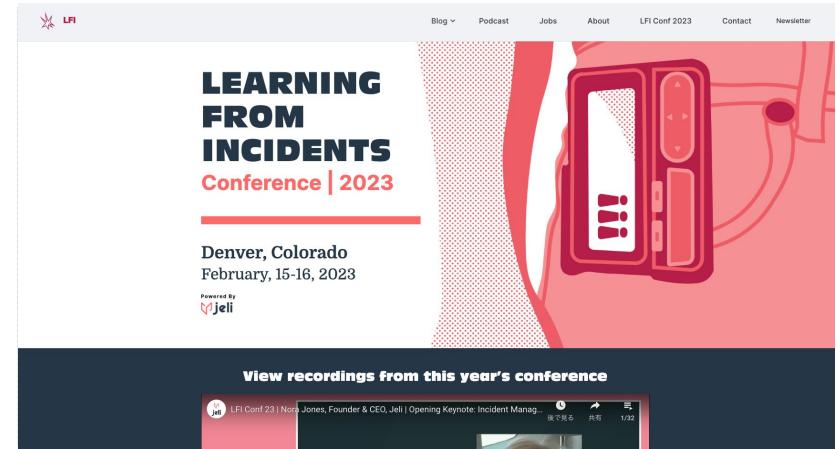
引用: <https://www.learningfromincidents.io/>

## The Incident Response Conference 2022



引用: <https://www.irconf.io/>

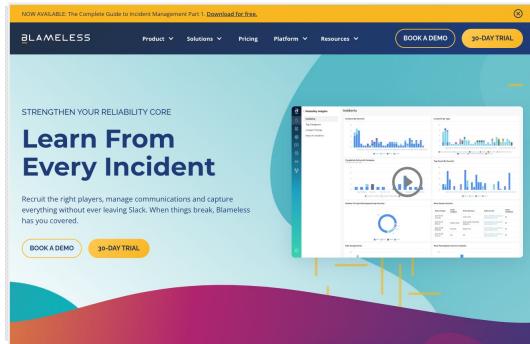
## LEARNING FROM INCIDENTS Conference 2023



引用: <https://www.learningfromincidents.io/learning-from-incidents-conference-2023>

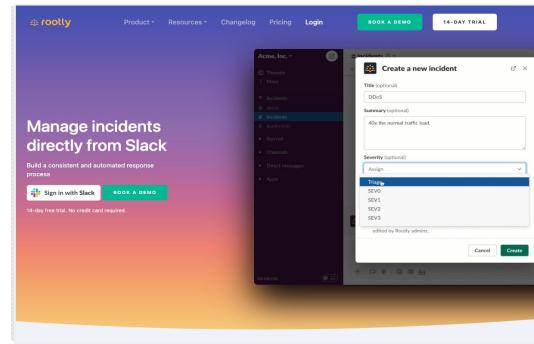
💡 SRE の文脈も含めた広義のインシデント（障害 + セキュリティインシデント）のカンファレンスのようです  
セキュリティインシデントをメインテーマにしたカンファレンスは他にもあると思います

## BLAMELESS



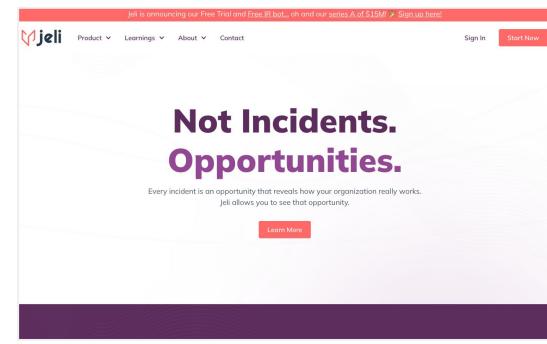
引用: <https://www.blameless.com/>

## rootly



引用: <https://rootly.com/>

## jeli



引用: <https://www.jeli.io/>

**BLAMELESS**

**rootly**

**jeli**

発表者が任意で選択したサービスになります

# incident.io

We've refreshed our Incident Management Guide for 2023! [Click here to get access](#)

[incident.io](#) Product Resources Pricing Careers [Start your free trial](#)

**Simple. Powerful. Effortless incident management**

With a beautifully simple interface, powerful workflow automation, and integrations with all your existing tools, prepare for incident management like never before.

[Start your free trial](#) [Book a demo](#)

SOME OF OUR HAPPY CUSTOMERS

引用:<https://incident.io/>



発表者が任意で選択したサービスになります

# Waroom

ドキュメント お問い合わせ ログイン 無料ではじめる

ベータ版提供開始

**インシデント対応のすべてを  
これ一つで改善・効率化**

Waroom はインシデント対応の準備から、対応中、対応後の  
全てに渡り SRE のプラクティスを用いて効率化できるツールです。

[無料ではじめる](#)

Topotail - インシデントを作成する

サービス: shop-backend ユーザーから誤って影響の出ているサービスを指定してください。

重要度: High

時間: 5分後 15分後 30分後 1時間後 2時間後 5時間後 10時間後 満了してください

チャンネル: Direct messages Add channels Slack Connect More

件名: #waroom Bot Add apps

キャンセル 作成

引用: <https://waroom.com/>



## Datadog

Datadog でのインシデント管理

引用: <https://www.datadoghq.com/ja/blog/incident-response-with-datadog/>



## PagerDuty Incident Response

Orchestrate the right response for every incident.

A Leader in Incident Management

引用: <https://www.pagerduty.com/platform/devops/incident-response/>

## Graphana Incident

Powerful incident management, built on top of Grafana

Grafana Incident makes responding to incidents faster by automating the routine tasks of incident management, which helps you focus on actually fixing the issue.

Help anyone start an incident

Reduce MTTR

Inform stakeholders faster

引用: <https://grafana.com/products/incident/>

# PagerDuty



発表者が任意で選択したサービスになります

# GMOペパボの インシデントマネジメント

## @sssbot <エスエスエススポット>

インシデントマネジメントを支援するSlack Bot を内製

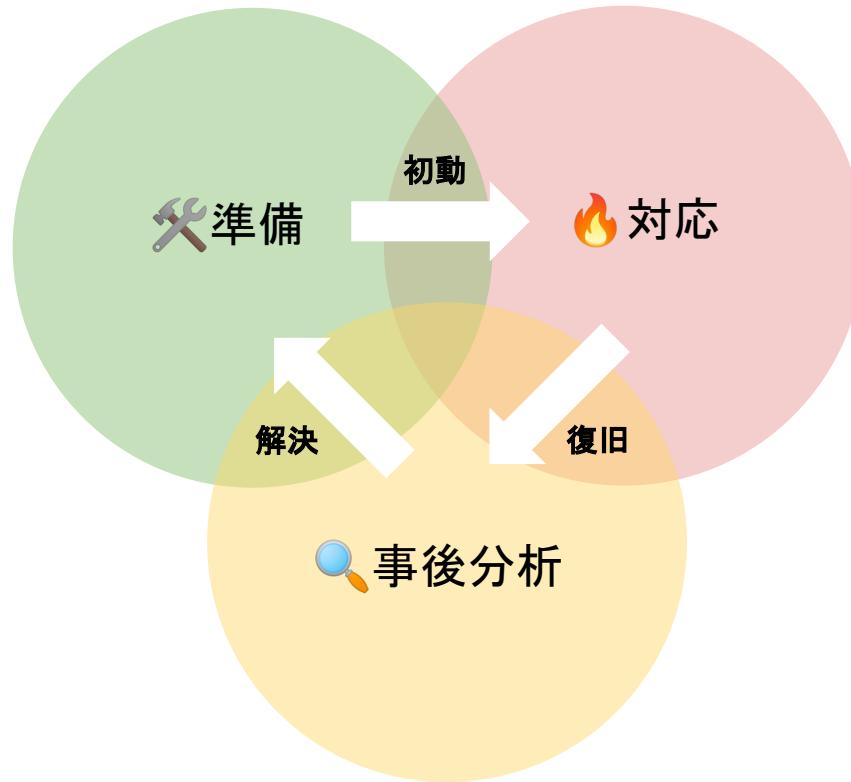
- ・ プロセスの標準化支援
- ・ コミュニケーションの支援
- ・ 分析・記録の支援

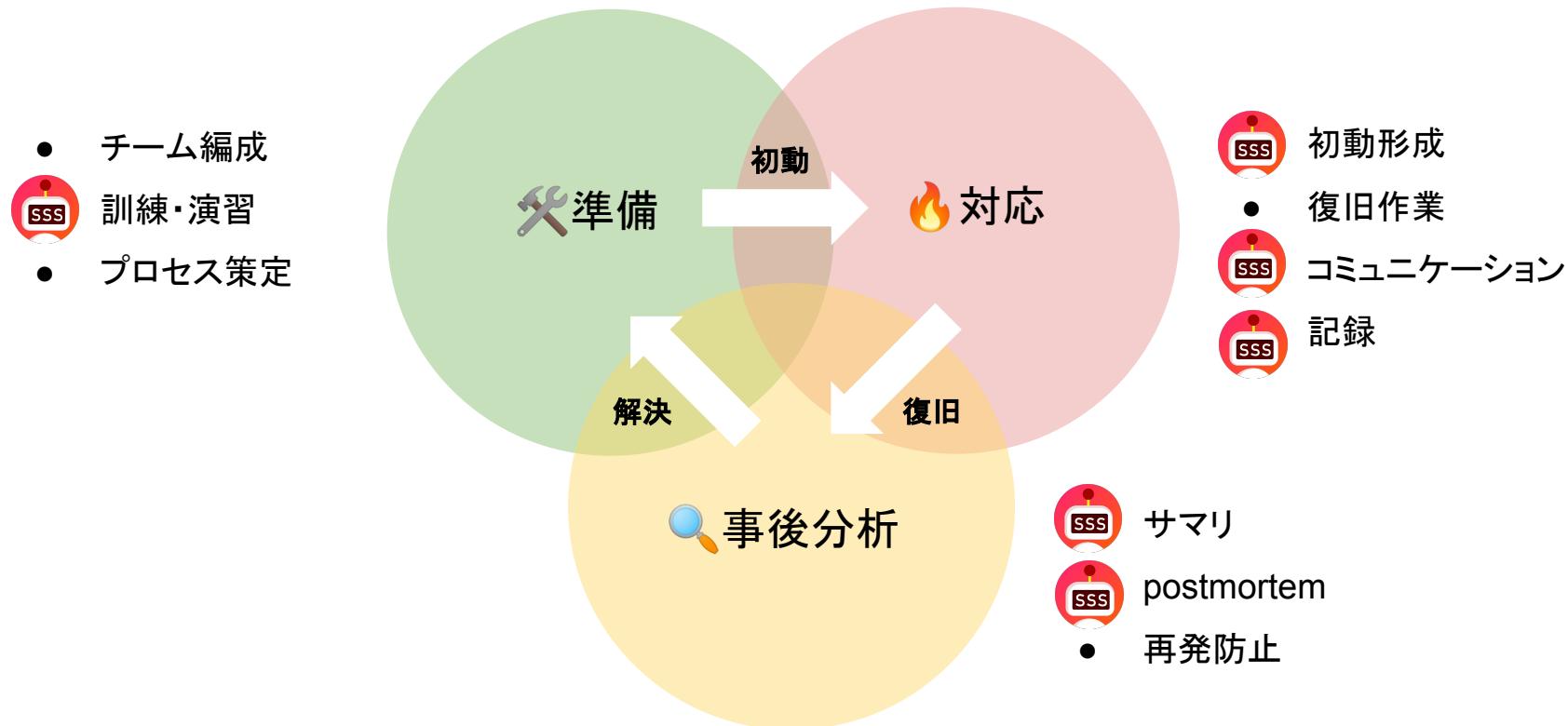


## CloudNative Days 2021での発表 インシデントレスポンスを自動化で支援する



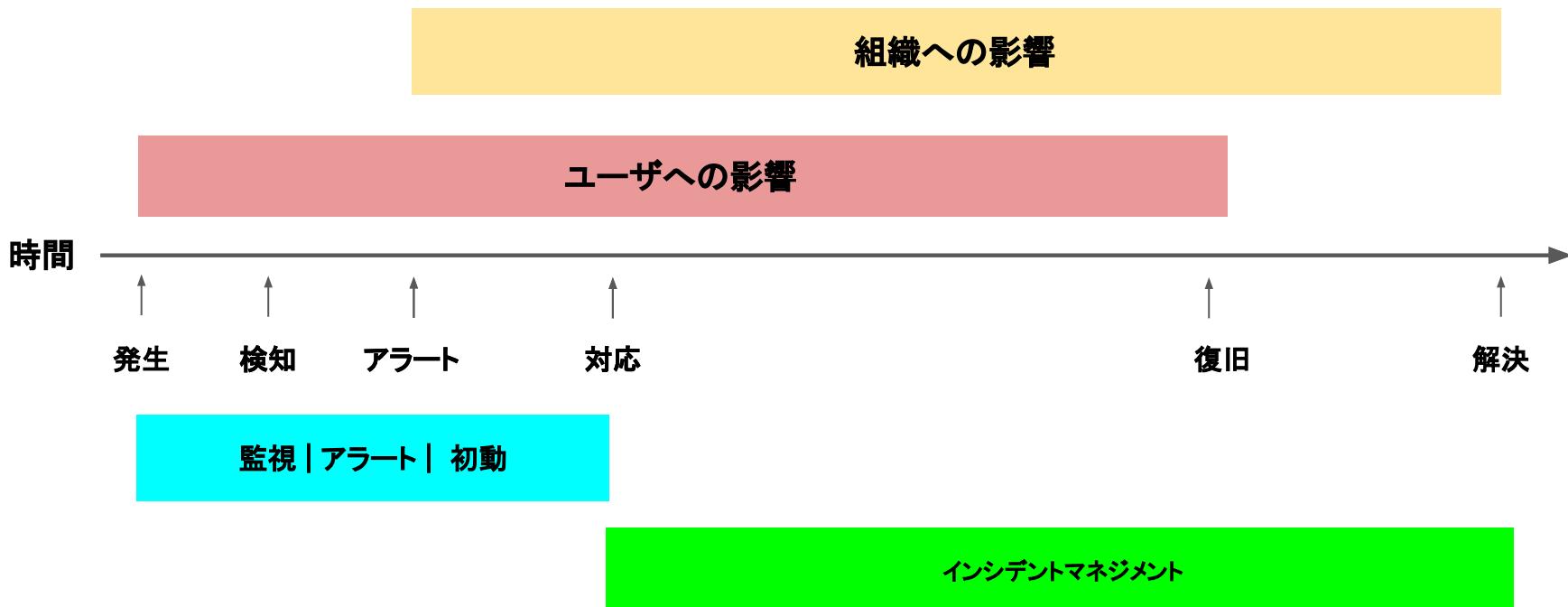
<https://speakerdeck.com/hiboma/insidentoresponsuwozi-dong-hua-dezhi-yuan-suru-slack-bot-deren-ji-ti-nasekiyuriteidui-ce-woshi-xian-suru>





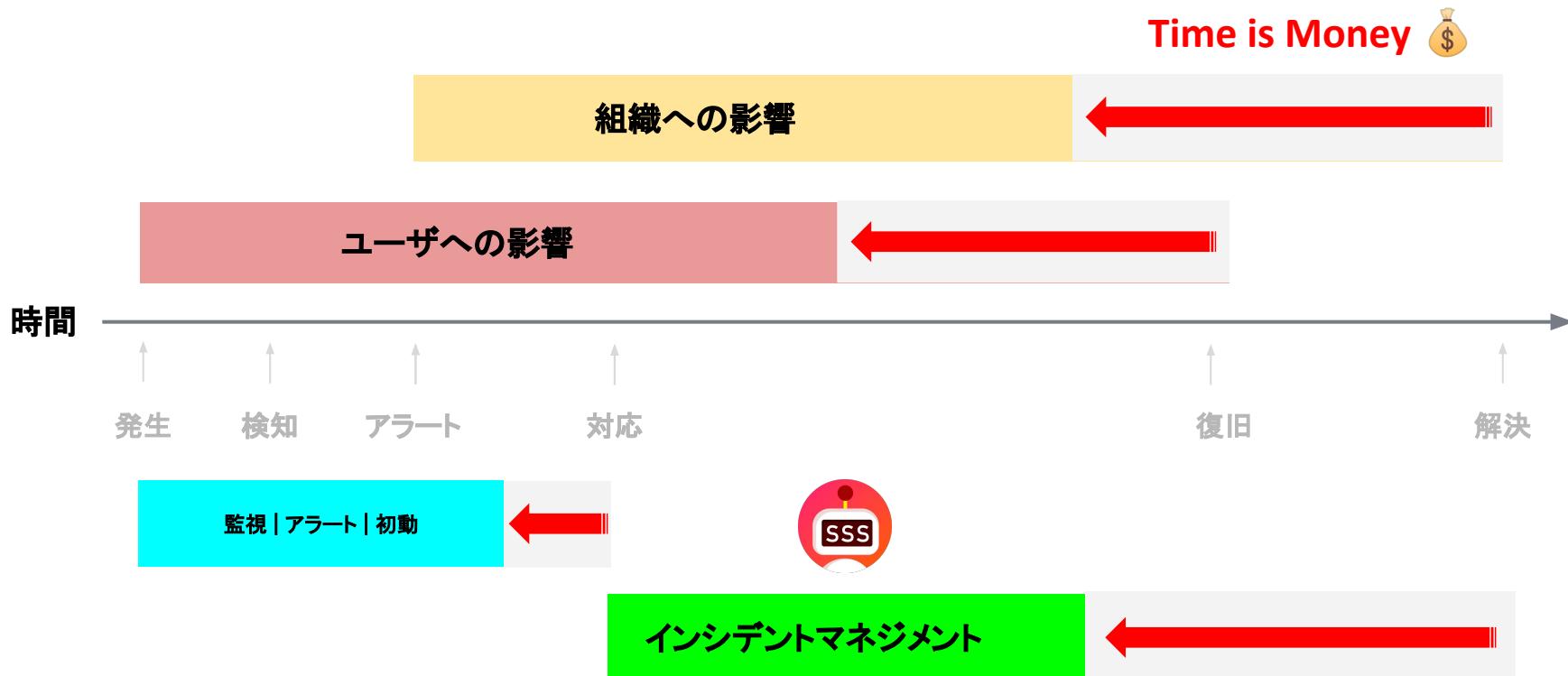
このモデル図は Brent Chapman さんの発表を元に、発表者が GMOペパボの実情に合わせて 改変・解釈した図としています

https://LFI Conf 23 | Brent Chapman | Incident Response and Incident Analysis: Two Great Tastes <https://www.youtube.com/watch?v=QAI3tF9eZek>



このモデル図は Brent Chapman さんの発表を元に、発表者が GMOペパボの実情に合わせて 改変・解釈した図としています

Incident Command for IT: What We've Learned from the Fire Department [https://www.usenix.org/sites/default/files/conference/protected-files/srecon18americas\\_slides\\_chapman.pdf](https://www.usenix.org/sites/default/files/conference/protected-files/srecon18americas_slides_chapman.pdf)



このモデル図は Brent Chapman さんの発表を元に、発表者が GMOペパボの実情に合わせて 改変・解釈した図としています

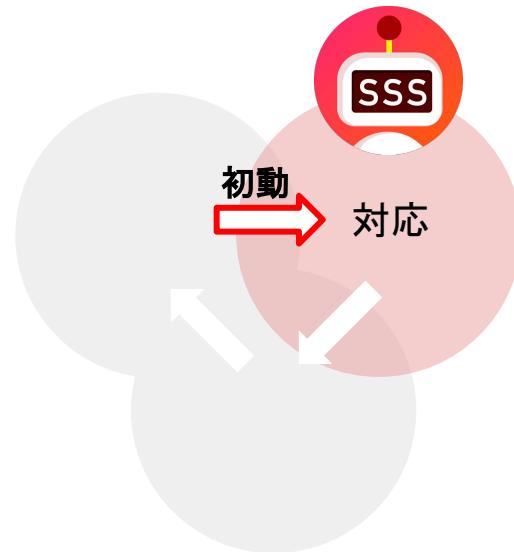
Incident Command for IT: What We've Learned from the Fire Department [https://www.usenix.org/sites/default/files/conference/protected-files/srecon18americas\\_slides\\_chapman.pdf](https://www.usenix.org/sites/default/files/conference/protected-files/srecon18americas_slides_chapman.pdf)



# @sssbot 初動の支援

## @sssbot が初動を形成、ニンゲンは復旧作業に集中

- ・ チャンネルの作成
- ・ 初動対応チームの招集
- ・ 組織内の連絡



## @sssbot を呼び出してチャンネルを作成する (1)

メンションで呼び出します

The screenshot shows a messaging interface with two messages from 'sssbot' and one from 'hiroya'. The first message from 'sssbot' contains a button labeled 'チャンネルを作る!'. The second message from 'sssbot' also contains a button labeled 'チャンネルを作る!'.

hiroya 21:40  
@sssbot

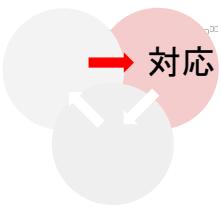
sssbot アプリ 21:40  
障害ですか?

sss セキュリティインシデントですか?

ヘルプの詳細は <https://.../wiki> に記載しています

チャンネルを作る!

チャンネルを作る!



## @sssbot を呼び出してチャンネルを作成する (2)

その時点でわかっている情報を添えて、フォーム入力してもらいます

sss チャンネルを作る

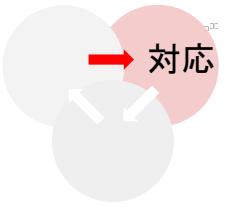
チャンネル名  
yapc-kyoto-20230319i  
チャンネル名は最大80文字までです

サービス  
other

いまいまの状況  
みんな、YAPC Reject Conf 楽しんでるかなー??? 明日も楽し  
みですね！

対応の温度感  
すでにヤバイ.緊急の対応をする

[① sssbotについてもっと詳しく](#) キャンセル 作成!



## チャンネル作成の通知をブロードキャストする

部門、サービス、職種でチャンネルが細分化されているので広く通知！

sssbot アプリ 11:07

障害対応チャンネルが作成されました

チャンネル #訓練\_nyah-20230220i

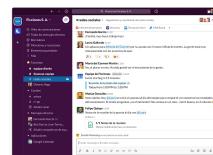
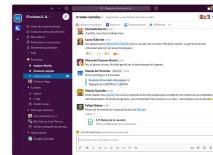
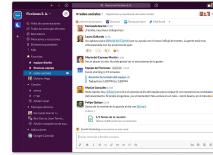
サービス nyah

温度感

YELLOW サービスに影響が出ている

いまいまの状況

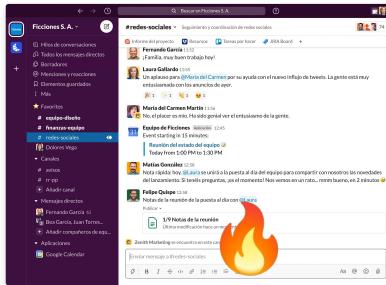
hoge のメールサーバなど重要なインスタンスを多数搭載する母艦がメモリ障害で凸落ちした可能性



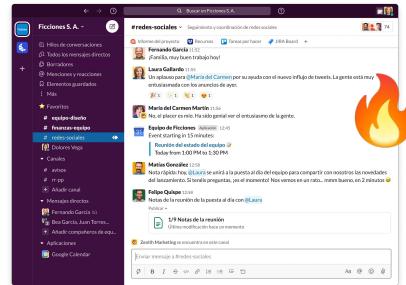
💡 スクリーンショットはインシデント対応訓練の Slack 通知であり、実際のインシデントではありません

# 1インシデント = 1チャンヤル

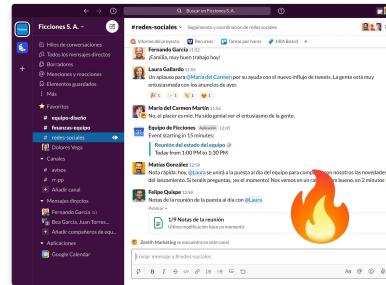
- 人間の認知負荷を下げたい
- 自動化で処理しやすい単位になる



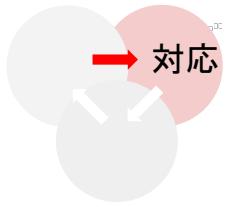
#サービスA-20200101i



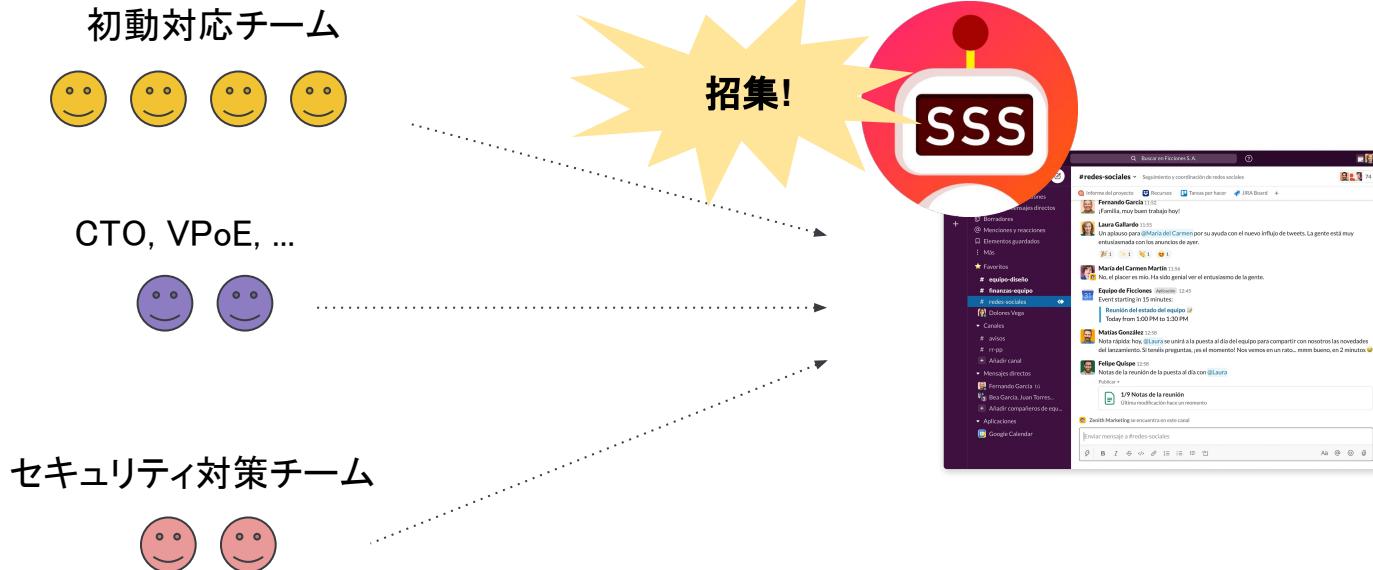
#サービスB-20200101i



#サービスC-20200101i



# @sssbot が初動対応チーム(\*) を invite する



💡 サービス、部門ごとに初動対応チームを編成しています。技術職、カスタマーサポート職、マネージャー職などが含まれる **slack** グループです。

スクリーンショットはSalesforce Collective: Collection Preview <https://salesforce.widencollective.com/c/raqrnql6> を用いた



# 対応の支援



## タイムキーパーで経過時間をお知らせする

インシデントのメタデータや TODO を表示する UI を兼ねる

タイムキーパーくん アプリ 10:41  
⌚ 初動から 15分 経過です

コマンド

---

事象レベル: 1  
ハンドラー: @hiboma  
❗ 検知の時刻を記録してください

💡 事象レベル: GMOペパボのインシデント対応マニュアル (非公開) にて定められた インシデントを 5段階評価するレベル

💡 インシデントハンドラー (コマンダー): インシデントの進行をリードする、一時的なリーダーロール

## タイムキーパーはコマンドランチャーの UI

コマンドを覚えず誰でも扱えるよう GUI のインターフェースを設ける

タイムキーパーくん アプリ 10:41  
初動から 15分 経過です

事象レベル: 1  
ハンドラー: @|

! 検知の時刻 を記録してください

コマンド

- 対応中のコマンド
- 検知の時刻を記録する
- 事象レベルをセットする
- ハンドラーになる
- 復旧の宣言を出す
- タイムキーパーを止める

復旧後のコマンド

- タグを記録する

## “復旧”できたら通知をブロードキャストする

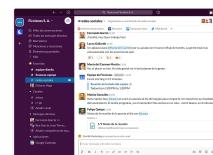
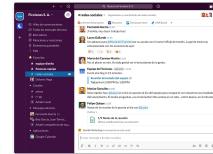
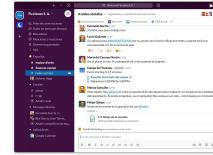
開けたら閉める。みんなに認知してもらうのが大事。



sssbot アプリ 12:54



#hosting-インシデント訓練20230301i 復旧しました!



💡 スクリーンショットはインシデント対応訓練時の Slack 通知であり、実際のインシデントではありません



# 事後分析の支援

## 事後分析で煩雑な処理を自動化して支援する

- postmortem (\*)ドキュメント作成の支援
- 記録の編集



💡 ペバボでは可用性・完全性・機密性が損なわれた状態を元に戻したことを「復旧」と呼んでいる



## postmortem のドキュメント作成と Pull Request 作成

sssbot で記録したデータで ドキュメント (markdown) の下書きを作ります  
チャンネルで したメッセージからタイムラインも自動生成します

sssbot アプリ 16:35

コマンド

@hiboma  
@matsusuke さんが postmortem を作る を押しました

postmortem の作り方

1 postmortem のタイムラインに載せたいメッセージをピン留め してください  
\* インシデントを復旧に導いた重要なメッセージをピン留めするとよいでしょう  
\* 例) 「○○さんがログから原因を見つけた」 「△△さんがコマンドを実行して復旧」

2 ピン留め したら、下のボタンを押して、Pull Request を出してください

Pull Request を出す



**ダッシュボードで過去のインシデントを参照する**

過去の事例や類似の事例を一覧できる。タグで過去の記録を編纂

インシデントの記録								
インシデント	id	98						
最近のインシデント	チャンネル	#nyah-20230309!						
月ごとのインシデント	サブインシデント	<a href="#">追加</a>						
	メインインシデント	<u>96 #other-20230307!</u>						
タグ	類型	障害						
ハンドラー	レベル	4						
チャンネル作った人	初動時の状況	SSL証明書発行時にページ認証で必要なファイルを指定ディレクトリに設置しない為、更新ができないくなる。SSL証明書発行時にページ認証で必要なファイルを指定ディレクトリに設置しない為、更新ができないくなる。SSL証明書発行時にページ認証で必要なファイルを指定ディレクトリに設置しない為、更新ができないくなる。						
Four Keys	対応後のサマリ							
ログアウト	タグ	<table><tr><td>tag-1</td><td><a href="#">削除</a></td></tr><tr><td>tag-2</td><td><a href="#">削除</a></td></tr><tr><td>tag-3</td><td><a href="#">削除</a></td></tr></table> <a href="#">追加</a>	tag-1	<a href="#">削除</a>	tag-2	<a href="#">削除</a>	tag-3	<a href="#">削除</a>
tag-1	<a href="#">削除</a>							
tag-2	<a href="#">削除</a>							
tag-3	<a href="#">削除</a>							
対応した人の記録								
チャンネル作成者	@user-1							
ハンドラー	@ssssbot	@user-1						

sssboard		Top > インシデントの一覧				
インシデント	サマリ	チャンネル		ステータス		サービス
		サマリ	チャンネル	ステータス	確認	
<input type="checkbox"/> switch view						
100	#sss-20230311i	サービス	種類	事象レベル	ステータス	タグ
		sss	sss	5	解決	データベース
初動時の状況			復旧後のサマリ			
DB の master で障害			対応後のサマリ			
			対応後のサマリ			
			対応後のサマリ			
タグ	検知	初動	招集	復旧	解決	ポストモーテム
ハンドラー	2023/03/11 17:42:33	2023/03/11 17:42:33	2023/03/11 17:42:33	2023/03/11 17:42:33	2023/03/11 17:42:33	#1
チャンネル作った人						
Four Keys	99	#30days-20230310i ← #other-20230307i	サービス	種類	事象レベル	ステータス
ログアウト	30days	障害	?	進行	DDoS	外部からの攻撃
初動時の状況			復旧後のサマリ			
原因不明のインシデント。対応中						
検知	初動	招集	復旧	解決	ポストモーテム	
	2023/03/10 17:42:33	2023/03/10 17:42:33	2023/03/10 17:42:33	?		?

💡 表示されているデータは、development 環境での seed です。実サービスのインシデントではありません



## 対応を“完了”したら 通知をブロードキャストする

全ての対応を完了して、チャンネルを/archive した際にも通知を出します。

sssbot アプリ 12:19  
#訓練\_it-support\_旧称shasys-20230228i が /archive されました。インシデントの対応、お疲れさまでした

チャンネル サービス  
#訓練\_it-support\_旧称shasys-20230228i other

初動時のサマリ  
会社PCを紛失してる

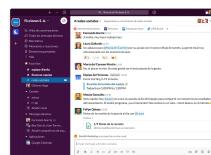
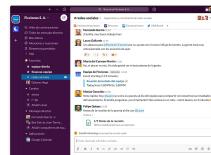
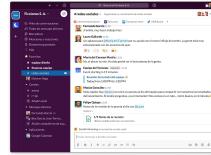
対応後のサマリ  
【訓練です】会社PCを紛失された。対象者： @

事象レベル  
0 ✓

対応にあたったみなさん、お疲れ様でした!

---

五人のユーザーアイコン



💡 スクリーンショットはインシデント対応訓練時の Slack 通知であり、実際のインシデントではありません

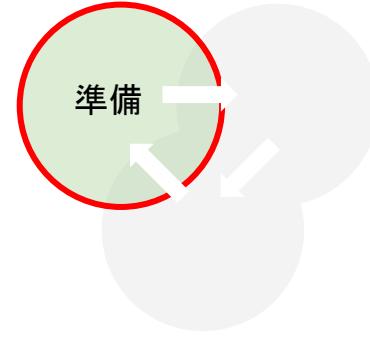


# 準備の支援

## GMOペパボのインシデント対応 訓練・演習

情報セキュリティ規定\* に基づき年一回以上 実施

- ・ 部門、サービスごとに訓練\*・演習\* を計画し実施する
- ・ @sssbot を用いて実施します



Software Design 2022 5月号 @takapi86 の記事もご覧ください!

注1) GMO ペパボの社内規定です（非公開）

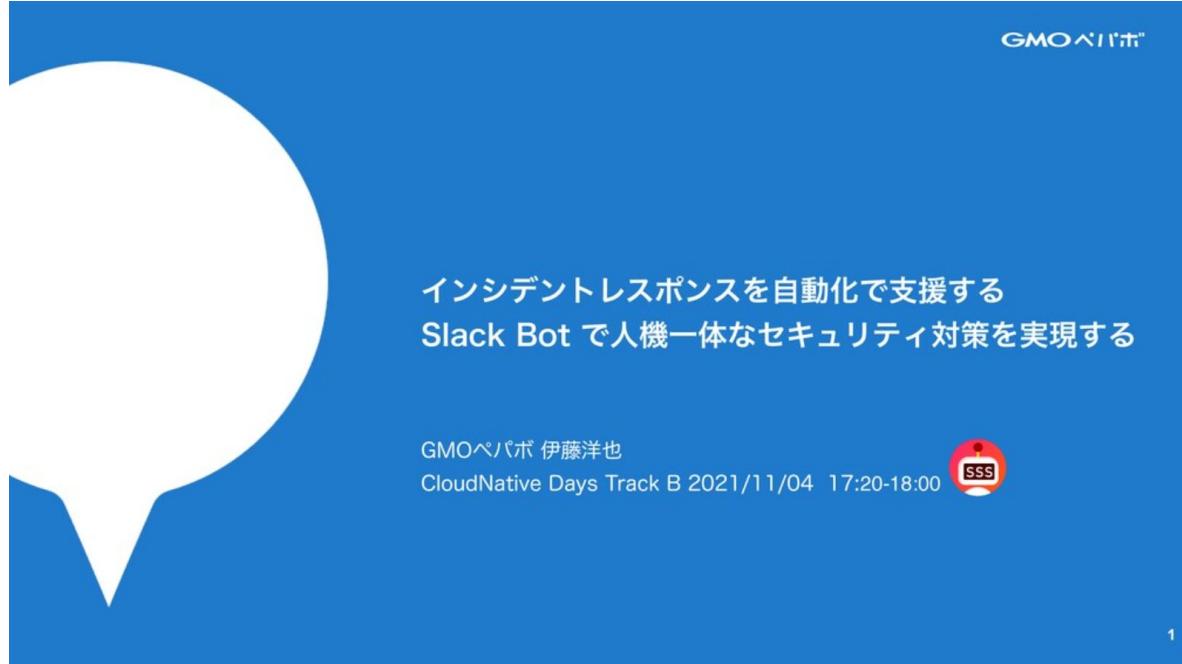
注2) 訓練 形式的な手続きやフローを習熟する目的で実施

注3) 演習 実践的なシナリオを想定した高度な内容で実施



# その他の機能

## CloudNative Days 2021での発表 インシデントレスポンスを自動化で支援する



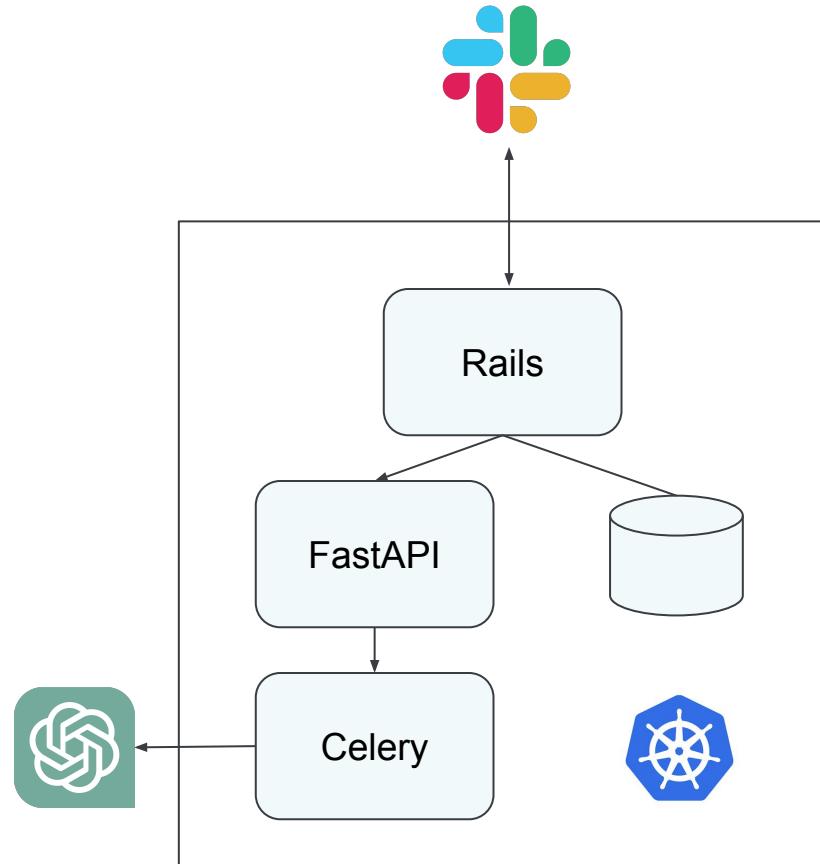
<https://speakerdeck.com/hiboma/insidentoresponsuwozi-dong-hua-dezhi-yuan-suru-slack-bot-deren-ji-ti-nasekiyuriteidui-ce-woshi-xian-suru>

# 実装 設計

## sssbot の実装

社内プライベートクラウド k8s で稼働

- Slack Bot + ダッシュボード パート
  - Ruby on Rails + slack-ruby-client
    - Slack Events API を利用
- ChatGPT パート
  - Celery + FastAPI



## Incident Command for IT

What We've Learned from Fire Department

### Incident Command for IT: What We've Learned from the Fire Department

USENIX SREcon18  
27 March 2018

PDF of these slides: <https://goo.gl/5C2M2d>

Brent Chapman

Brent@GreatCircle.com  
@brent\_chapman

# Great Circle

Copyright © 2018, Great Circle Associates, Inc. All Rights Reserved.

引用 [https://www.usenix.org/sites/default/files/conference/protected-files/srecon18americas\\_slides\\_chapman.pdf](https://www.usenix.org/sites/default/files/conference/protected-files/srecon18americas_slides_chapman.pdf)



@brent\_chapman

## Incident Response and Incident Analys Two Great Tastes

**Brent Chapman**  
Founder & Principal  
Great Circle Associates



引用 <https://www.youtube.com/watch?v=QAl3tF9eZek>

## @sssbot の DNA: Brent Chapman さんから学ぶ

チャットを活用するためのプラクティスが盛りだくさん

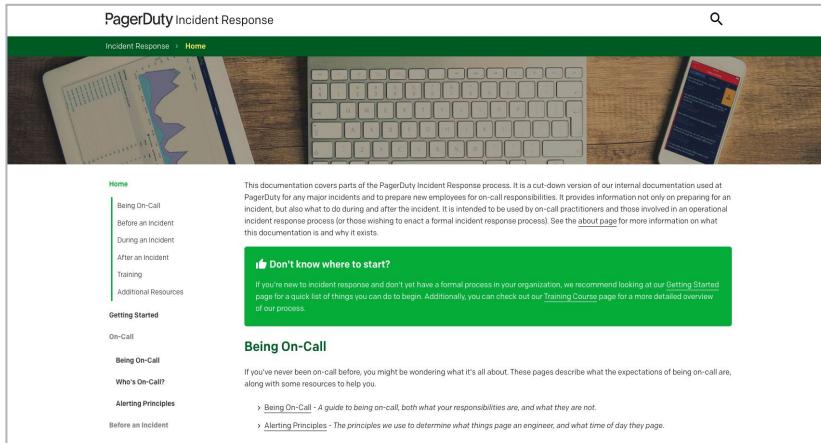


- チャンネルの運用方法
  - 例) 1チャンネル1インシデント、名前の付け方
- チャットコミュニケーションの回し方
  - 例) 自分が何をやっているかテキスト、スクショ、リンクを貼って声をあげよう
- インシデント時の組織体制
  - 例) 平時と緊急時のリーダーシップは別で考えよう

3象現やタイムラインのモデルも Brent Chapman さんのエントリの内容を元にしています。ありがとうございます ....

## @sssbot の DNA

## PagerDuty Incident Response



The screenshot shows the homepage of the PagerDuty Incident Response documentation. At the top, there's a navigation bar with 'Incident Response' and 'Home'. Below the header is a large image of a laptop, keyboard, and smartphone displaying incident response interfaces. The main content area has a dark green sidebar on the left containing links like 'Home', 'Being On-Call', 'Before an Incident', etc. The main content area features a section titled 'Don't know where to start?' with a call-to-action button. Below it is a 'Being On-Call' section with descriptive text and links to 'Being On-Call - A guide to being on-call, both what your responsibilities are, and what they are not.' and 'Alerting Principles - The principles we use to determine what things page an engineer, and what time of day they page.'

引用 <https://response.pagerduty.com/>

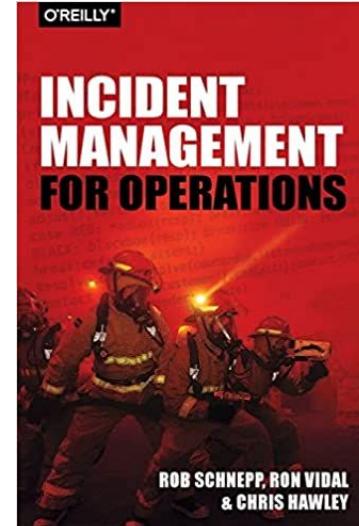
## @sssbot の DNA



引用: <https://www.oreilly.co.jp/books/9784873117911/>



引用: <https://gihyo.jp/book/2020/978-4-297-11265-3>

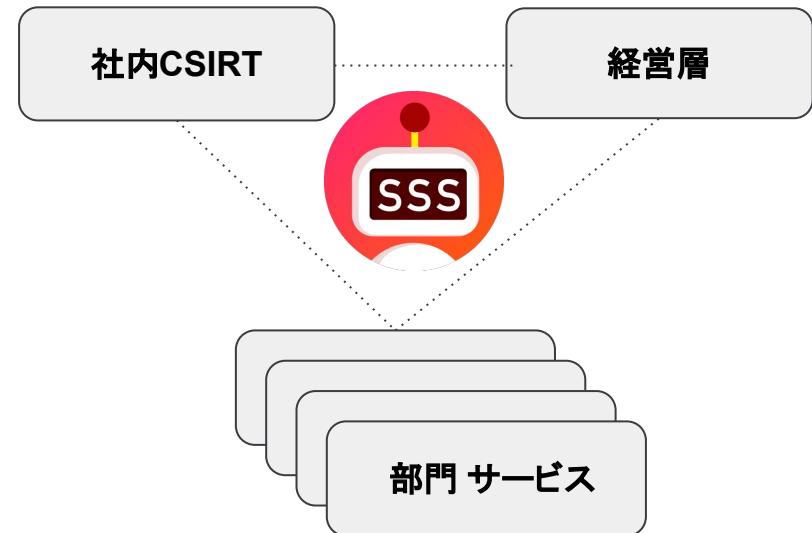


引用: <https://www.oreilly.com/library/view/incident-management-for/9781491917619/>

# 評価 課題

## @sssbot で改善できたこと

- ・ 部門やサービスを超えてのプロセスの標準化
- ・ CSIRT\* や 経営層への情報共有の促進



## @sssbot を使っても、なお残る課題感

やっぱり 事後分析のプロセスが重たい ...

- ・ サマリをまとめる
- ・ postmortem のドキュメントを書く
- ・ postmortem のレビューを進行する
- ・ アクションアイテム\* を出す (最重要)

「後でやろう」となりがち



注) postmortem の文脈でなければ、再発防止策と呼ぶでしょう。

## 改善案: ChatGPT API でインシデントのサマリを生成

3日前に作ったばかり



hiboma (開発環境) 22:09

@sssbot-development サマリを考えて



sssbot-development アプリ 22:09

はい。サマリを考えてみます。しばらくお待ちください 🍽

【サマリ】

- 事象レベル: 1 (最高レベル)
- 発生した問題: DBのmasterで障害が発生
- 復旧の時刻: 2023年3月16日21時47分19秒
- 影響の範囲: 不明
- 対応の内容: インシデントレスポンステムを招集し、復旧作業を実施。事象レベルが1に引き上げられたが、復旧宣言が出された。

llama\_index の SlackReader + GPTSimpleVectorIndex + ChatGPTLLMPredictor で作っています

1チャンネルに 1インシデントの記録が集約されるので、チャンネルのメッセージを丸ごとインデックスして扱えば良い

## AI (ChatGPT API) + インシデントマネジメント支援 = 楽しみ

- ・ インシデントログのデータ活用で、明るい未来が見える
- ・ 初動・対応フェーズでの活用も模索したい
  - ・ ChatGPT API の処理速度が上がれば、準リアルタイムでも支援できるだろう
  - ・ 支援だけでなく「インシデント 解決方法の提案」も実現可能



# Thank You!

「ご静聴ありがとうございました」「We're hiring」などに言い換えても。

GMOペパボ

# 見送りスライド

## インシデントマネジメントのシステム内製の pros / cons

### pros

- 組織の体制やプロセスに準じた機能を提供
- 同僚からフィードバックを受けてすぐUI / UX 改善

### cons

- 作り込み度合いをどこまでやるか
  - 私がWeb UI の実装に弱いという話も ...



## 最近の課題感

インシデントが同時多発するとグシャっとなる

- 例) 社外連携している SaaS や IaaS で障害 🔥
  - ペパボ内の複数サービスでインシデントチャンネルが同時にたつ
  - チャンネルを超えて情報共有や指示出しが進めにくい



Saas / Iaas

