cookpad

2021.7.9 (Fri)
Internet Week

リモートワークを支える
社内セキュリティ基盤の構築と運用

クックパッド株式会社
コーポレートエンジニアリング部 セキュリティグループ
水谷 正慶

自己紹介

水谷 正慶 (@m_mizutani)

- **博士（政策・メディア）**
- **2011.4 ～ 日本IBM**
  - SIEMなどセキュリティ関連の研究開発
  - SOCアナリスト
- **2017.11～ クックパッド**
  - 技術部セキュリティグループ
  - 社内のセキュリティ基盤の構築・運用
  - CSIRT・情報セキュリティ委員会業務など

本日ご紹介する内容

- **クックパッド内における社内システム構築・運用の体制**
- **リモートワーク環境下でのリスクと課題**
  - 不審なアクセスに対する備え
  - トラブル・インシデント発生時への備え
- **現在クックパッドが取り組んでいる対応全般についてご紹介**
  - 今回はシステムや取り組みなど全般を「セキュリティ基盤」としています

クックパッドにおける
社内システムの概要

私たちのミッション

「毎日の料理を楽しみにする」

Make everyday cooking fun!

ミッション実現に向け、各領域でさまざまな事業に挑戦しています。

つくり手をふやす

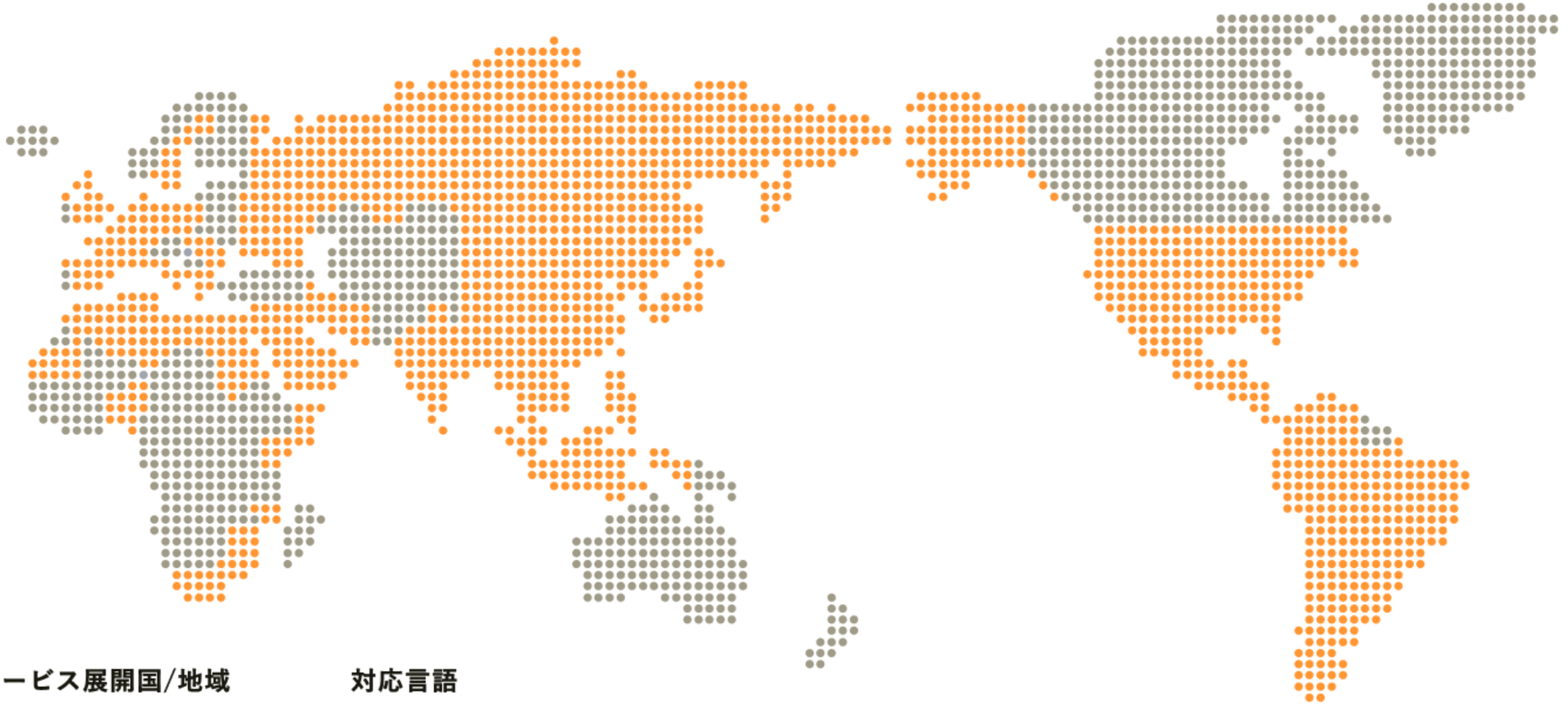
cookpad　Oicy　cookpad Live

毎日の料理の課題を技術で解決し、つくるハードルを最小限に。つくる楽しさは最大限に。毎日の料理を楽しみにし、つくり手を増やします。

つくり手をつなげる

cookpad mart　komerco

料理、道具、食材など、さまざまなつくり手をつなげることで、すべてのつくり手が継続的に収入を得ることができる仕組みをつくります。



サービス展開国/地域

74カ国/地域

対応言語

32言語

料理は、万国共通の習慣。だから、私たちの挑戦は国内にとどまりません。
英国ブリストルに構えたグローバル本社を起点に、世界各国へとクックパッドを広げていきます。

※ 2020年9月30日時点

社内サービスを構築する上での原則

- **1) リモートワークが「特別」にならないようにする**
  - Before コロナからの原則
  - 以前からリモートワークも一部認められていた
  - グローバルのチームも原則同じシステムを使っている

- **2) 社内ITチームの持ち物を少なくする**
  - 物理サーバの管理負担軽減
  - アプリケーションのメンテナンス負担軽減
  - DR機能をサービスプロバイダへ移譲

社内向けサービスの構成概要

- **原則としてSaaSを使う**
  - ドキュメント管理：Google Drive、OneDrive
  - コミュニケーションツール：Gmail、Slack
  - サービスマネジメントツール：ServiceNow、Workday、Zendesk
  - リモートデスクトップ：Amazon WorkSpaces
- **自分たちでサーバ管理する必要があるものはAWS上へ**
  - ファイルサーバ、DHCPサーバ、AD/DCサーバ
- **認証認可は原則SSOおよびMFAを利用**
  - Azure AD、Google Sign-inなど
- **なるべくVPNに頼らない**
  - 帯域・遅延の問題

オフィス・オンプレミスで完結している環境との違い (1/2)

- **ネットワークレイヤーを信頼することができない**
  - 世界中どこからでもアクセスがあると仮定
  - 接続元を制限するのは管理の点から現実的ではない

- **利用制限するタイプの対策をとりにくい**
  - プロキシなどによるネットワーク接続先制限は現実的ではない
  - CASBなどは遅延の問題＋開発環境への影響大により未使用
  - フィッシングやマルウェア感染のリスク

オフィス・オンプレミスで完結している環境との違い (2/2)

- **（物理的に）近くに同僚がいない**
  - 何かあったときの相談のハードルがあがる
  - 困っている同僚がいても周りが気づけない
  - トラブル時にすぐ本人＆端末へアクセスできない

想定する脅威と課題

- **想定する脅威**
  - Eメール、Webサイトを通じたエンドポイントからの侵入
  - クラウドサービスを通じた侵入

- **脅威に対抗するための課題**
  - 不審なアクセスに対する備え
  - トラブル・インシデント発生時への備え

cookpad

課題(1/2)
不審なアクセスに対する備え

外部からの不正アクセスへの対応

- **外部（第三者）≠社外ネットワーク**
  - ネットワーク情報から第三者かどうかの判断は困難
- **MFAを利用しても不正アクセスは防ぎきれない**
  - フィッシングサイトによるOTPの窃取
  - PCのマルウェア感染による認証情報の窃取
- **不正アクセスの兆候があった場合**
  - 迅速に気づけるようにする
  - 気づいた事象が実際のリスクであるか調査できるようにする

対応策

- 各サービスにおける不審な挙動を検出
- 防御だけでなく監視を多重化
- 各サービスのログを俯瞰して調査できる基盤の構築
- 通報プロセスを簡略化と脅威についての周知

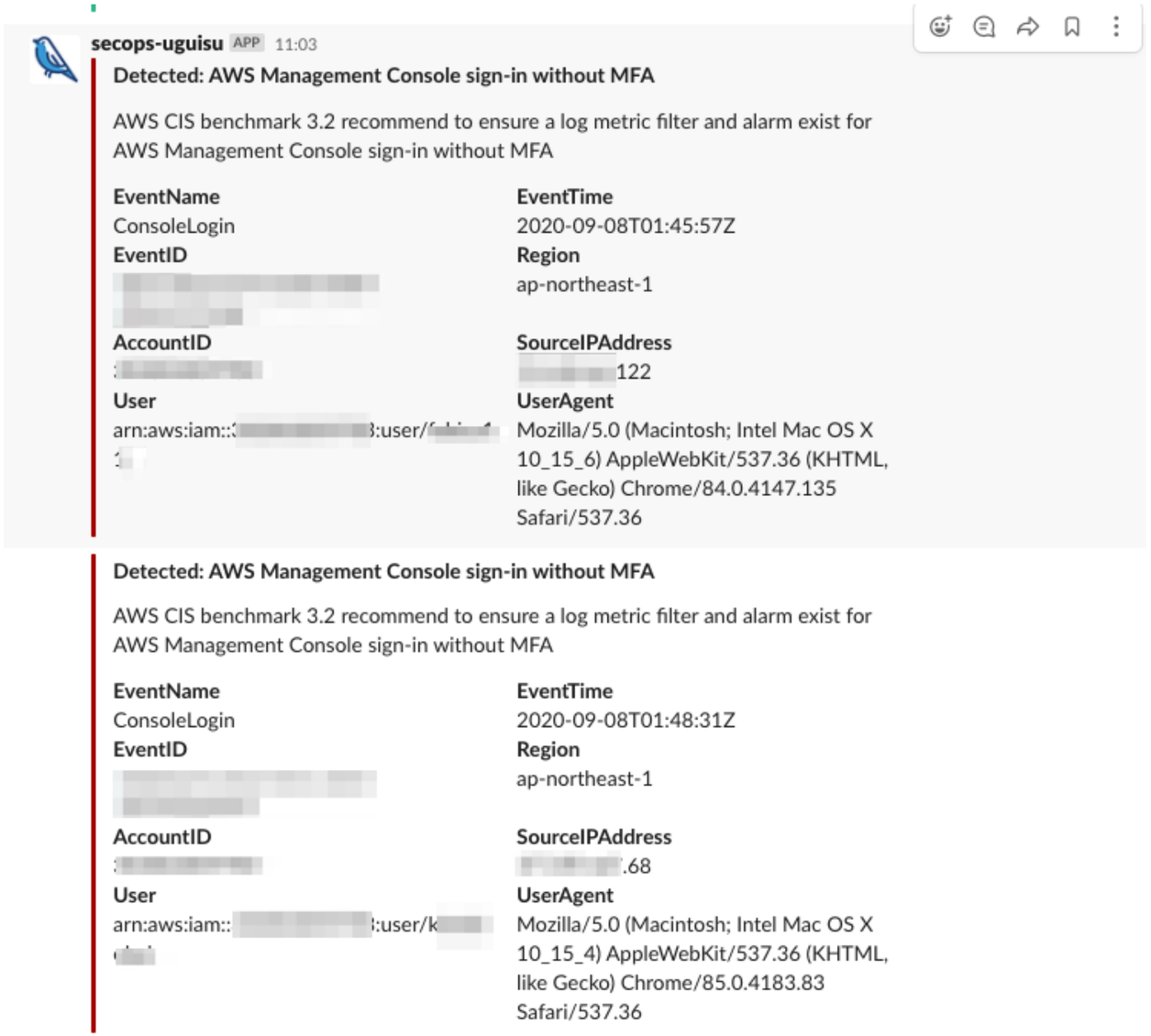
対策(1/4) 各サービスにおける不審な挙動を検出

- **クラウドサービスへの不審行動検出機能を活用する**
  - AWS (GuardDuty), Google (Audit log) など
  - 追加の作業など特になく利用可能

- **クラウドサービスの利用状況を監査する**
  - 全てのログを監視するのは不可能なので監視する対象を絞る
  - CIS (Center for Internet Security) Benchmarks を参考
  - 自社のポリシーなどと照らし合わせて「明確に禁止していないがあまり望ましくない行為」を監視

クラウドサービス監視：Uguisu

- **AWSの注目すべきイベントをSlackに通知**
  - CloudTrail（監査ログ）から該当イベントを抽出
  - CIS benchmarksを参照
    - https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-cis-controls.html
  - 命名の由来は“鶯張り”



https://github.com/m-mizutani/uguisu

対策(2/4) 防御だけでなく監視を多重化

- **監視するポイントを複数にすることで検知漏れを防ぐ**
  - 横の展開：複数の業務用サービスでの監視
  - 縦の展開：エンドポイント → 業務用サービス → 自社サービス基盤

- **監視は攻撃側から観測できないため多重化は有用**
  - 例えば「”標的型”ランサムウェア攻撃」はステルス性が低いと言われている
  - 監視ポイントが多いことで、痕跡を残せる可能性が高くなる
  - ただし、アラート発報数が増加すると監視の負担が大きくなるため対策は必要

参考「SOARによるセキュリティ監視業務の効率化とSecOps」 CODE BLUE 2020

https://speakerdeck.com/mizutani/soar-and-secops

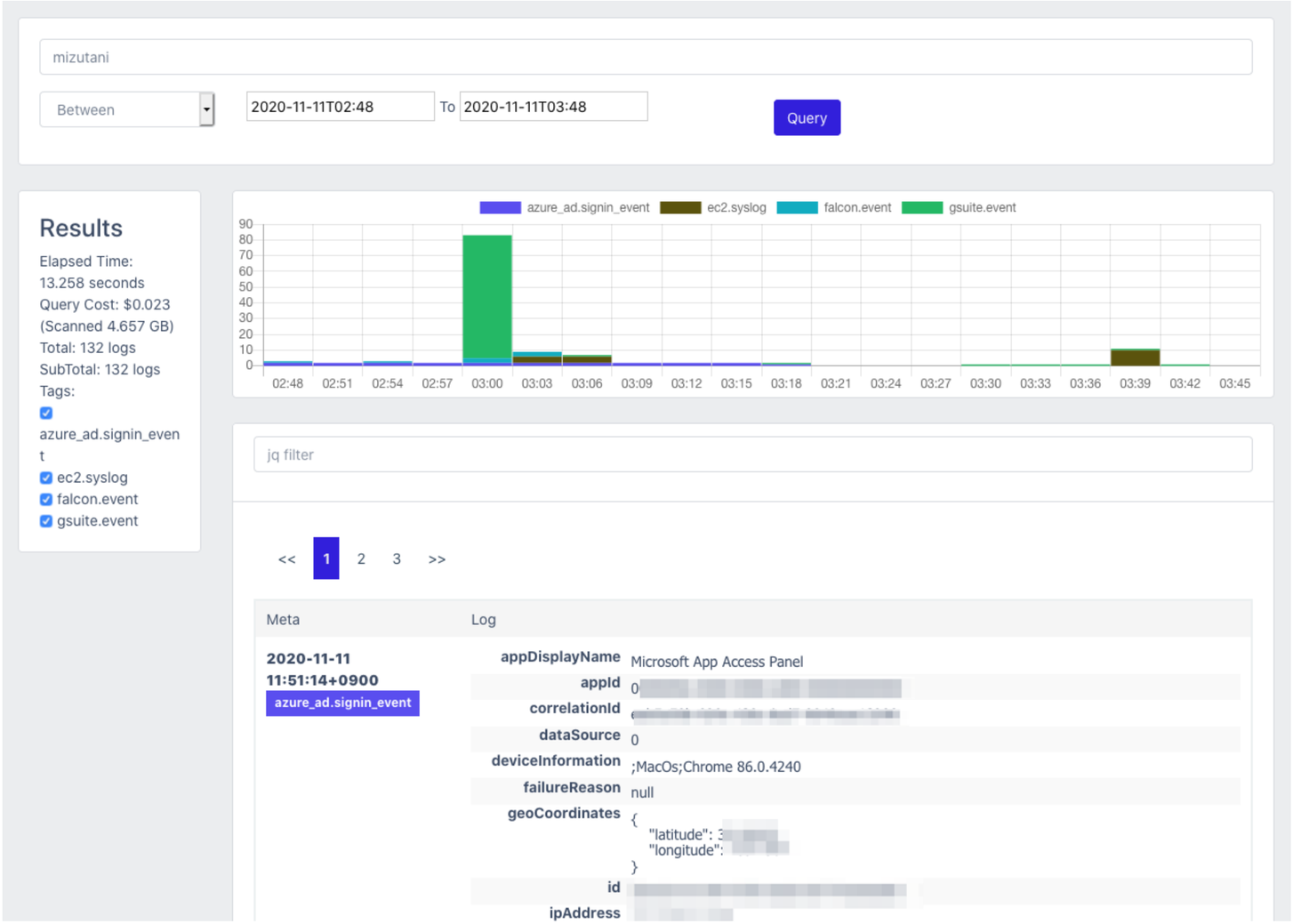
対策(3/4) 各サービスのログを俯瞰して調査できる基盤の構築

- **サービスごとにログが分断されていると調査の負担が増加**
  - サービスごとの管理コンソール上からのみログにアクセス可能などの状況
  - 分断されていることで見落としなどのミスが発生

- **各サービスのログを検索できる統一的なインターフェースが必要**
  - 速やかに関連するログの収集が可能
  - ログの関係性調査や時系列調査が容易になる

セキュリティログ管理基盤：Minerva

- **AWS Athenaを利用したログ検索基盤を構築・運用**
  - 全文検索システム
  - 社内サービス・エンドポイントログ・AWSログなどを検索可能
  - コスト：月額$300程度

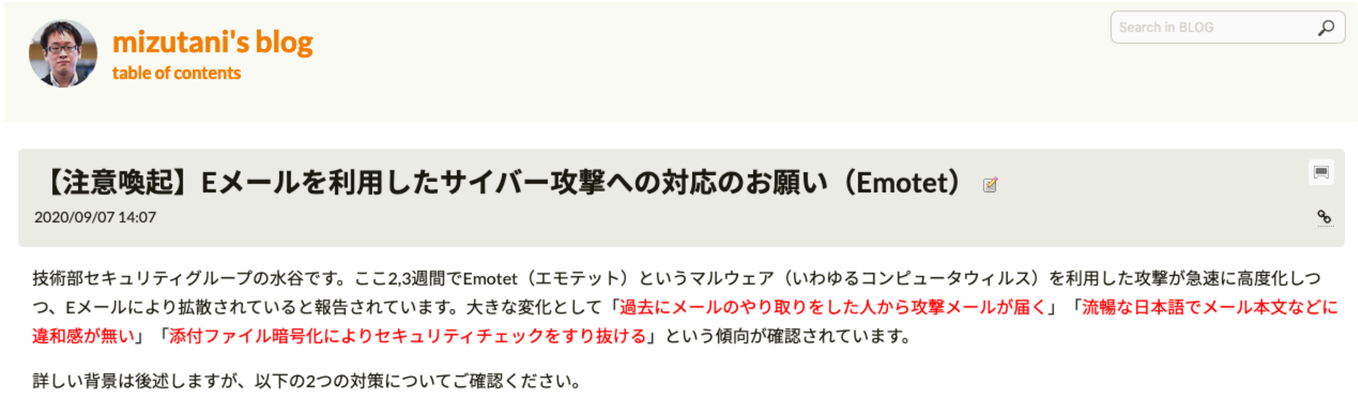


参考「Amazon Athena を使ったセキュリティログ検索基盤の構築」

https://techlife.cookpad.com/entry/2019/11/21/073000

対策(4/4) 通報プロセスを簡略化と脅威についての周知

- **社内のメンバーがなにかに気づいた際の通報のハードルを下げる**
  - 通報窓口の集約：インシデントの種類に依存しない
  - 通報内容の簡略化：不確かな情報や誤検出の可能性があっても良いことを周知
- **対応が必要な脅威について周知する**
  - 全ての脅威に対して注意を払うのは難しいのでリスクの高い脅威に絞る
  - 「水際対策」ではなく、あくまで検出・回避の可能性を高めるのを目的とする



社内ブログでの共有

cookpad

課題(2/2)
トラブル・インシデント発生時への備え

インシデント発生時の速やかな対応が必要

- **筐体（特にPC）に対して物理的にアクセスできないため対応が困難**
  - PCの本体を直接操作して調査できない
  - 記憶媒体（ディスクなど）の低レイヤなアクセスによるデータの救出やフォレンジックができない
- **物理的にアクセスするためには大きな遅延が発生**
  - 影響範囲などの調査の遅れ
  - 当該PCを利用していた社員の業務遂行に対する支障

対応策

- 業務データおよびシステム関連ログをクラウドへ保存
- 遠隔インシデントレスポンスの実現

対策(1/2) 業務データおよびシステム関連ログをクラウドへ保存

- **PC上に業務データを極力残さないようにする**
  - Google Drive File Streamなどを使うことで業務データをアップロード
  - 対応ファイルの編集などはブラウザ上で完結させる
- **クラウド上でデータ保護することでインシデントに対する耐性が高まる**
  - ローカル・クラウド上のデータを破壊されても回復可能
  - ローカルのデータを捨てやすいので筐体の交換も容易
- **フォレンジックに利用するログもクラウド上へ**
  - CrowdStrike Falcon (EDR, Endpoint Detection & Response) で取得したログをクラウド側で保持することで追跡のための情報を常に保全
  - 筐体内のディスクをフォレンジックすることなく影響範囲の推定が容易に

対策(2/2) 遠隔インシデントレスポンスの実現

- **遠隔から（特権的に）何かあったPCに対して操作できる体制**
  - Zoomのリモートコントロールでトラブル対象のPCを操作
  - CrowdStrike Falconの遠隔対応機能を利用
    - プロセスの停止やファイル削除だけでなく、プロセスメモリの抽出やファイルの隔離などが可能
  - 接続元地域に限らず対応可能（ただしタイムゾーンなどの問題はある）

まとめ

まとめ

- **リモートワーク対応環境とはリモートワークのためだけのものではない**
  - リモートワークな状況でなくてもセキュリティ対策の強化や効率化につながる

- **自分たちの組織にとって必要なことを見極め、自らで対応していく**
  - リモートワーク環境ならではのリスクは存在しているが対応可能
  - 対応するための道具は世の中に揃っている
    - クラウドサービス、EDR、各種ツール、など
  - 全体のデザインを自分たちで考え、必要なものを構築していく

Thank you