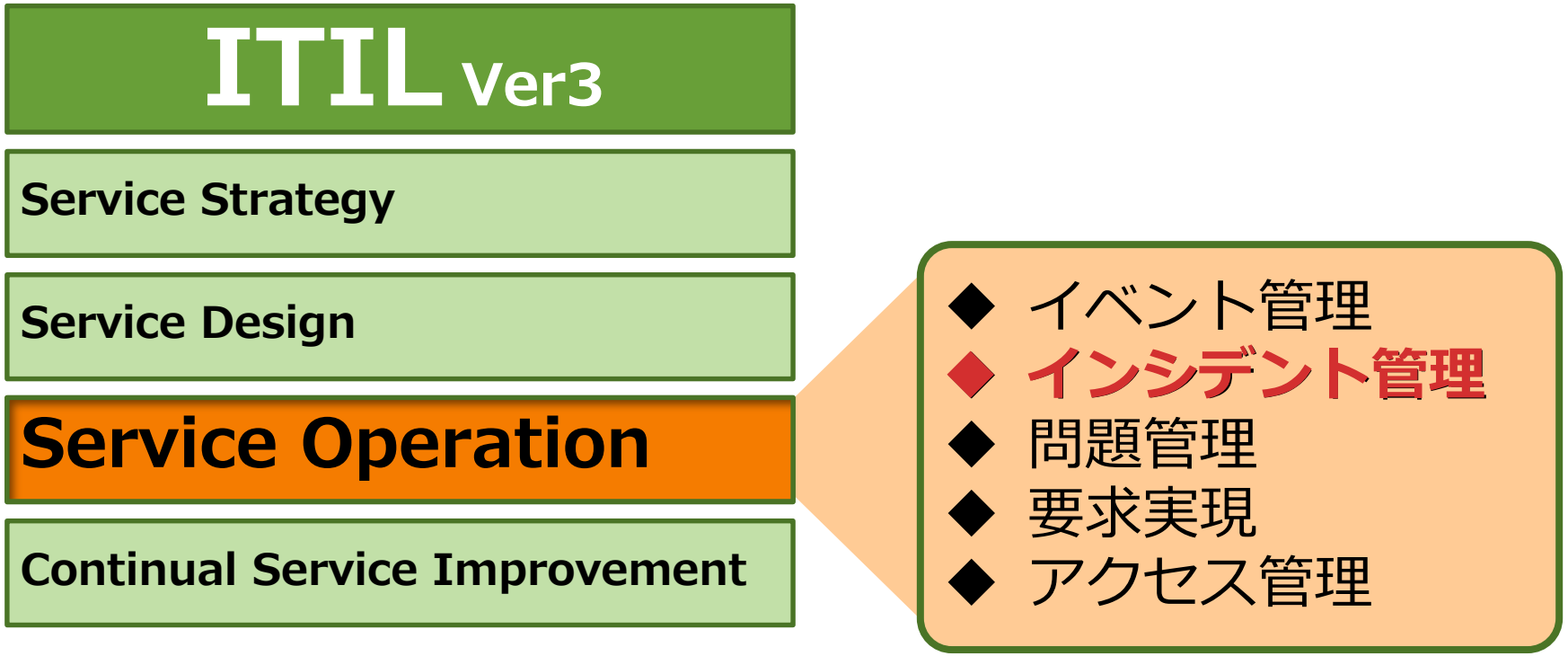
監視システムからの膨大なアラートを自動的に集約/判断し、インシデント管理、ジョブ管理に自動連携する方法

cybertrust

公開

インシデント管理

サービスオペレーションのプロセスの１つ



インシデント管理とは

目　的

インシデントにより中断されたITサービスを早急に復旧させ、ビジネスの負のインパクトを最小限にすること

インシデント管理のプロセス

1　検知と記録
2　分類と初期サポート
3　調査と診断
4　解決と復旧
5　インシデントのクローズ

プロセスとしてはシンプルではありますが・・・・確実に行うことは大変です。
（ITサービスの運用を円滑に回す為の重要なポイントとなる為、しっかりと行う必要があります。）

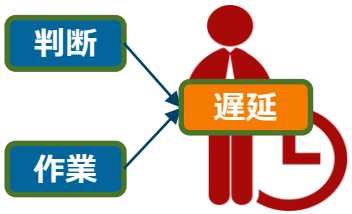
その為には、専用のツールを導入することも解決の１つとなります。

実際に現場は・・・・

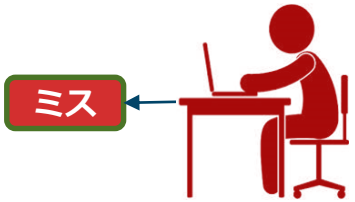
【課 題】

✓メール電文を見て障害対応の必要性を判断 → 遅延
✓メール電文からチケットに必要な項目を転記 → 記述ミス
✓チケット起票を優先すると対応着手が遅れる → SLA違反へ
✓障害対応の優先で対応状況がわからない → 管理に支障

運用業務の自動化で期待できる効果

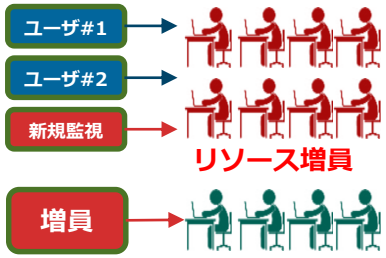


1.業務の効率化



2.人的ミス削減

3.運用プロセスの定着



4.サービス拡大に対応

インシデント管理システムを使うと・・・・

【効果】

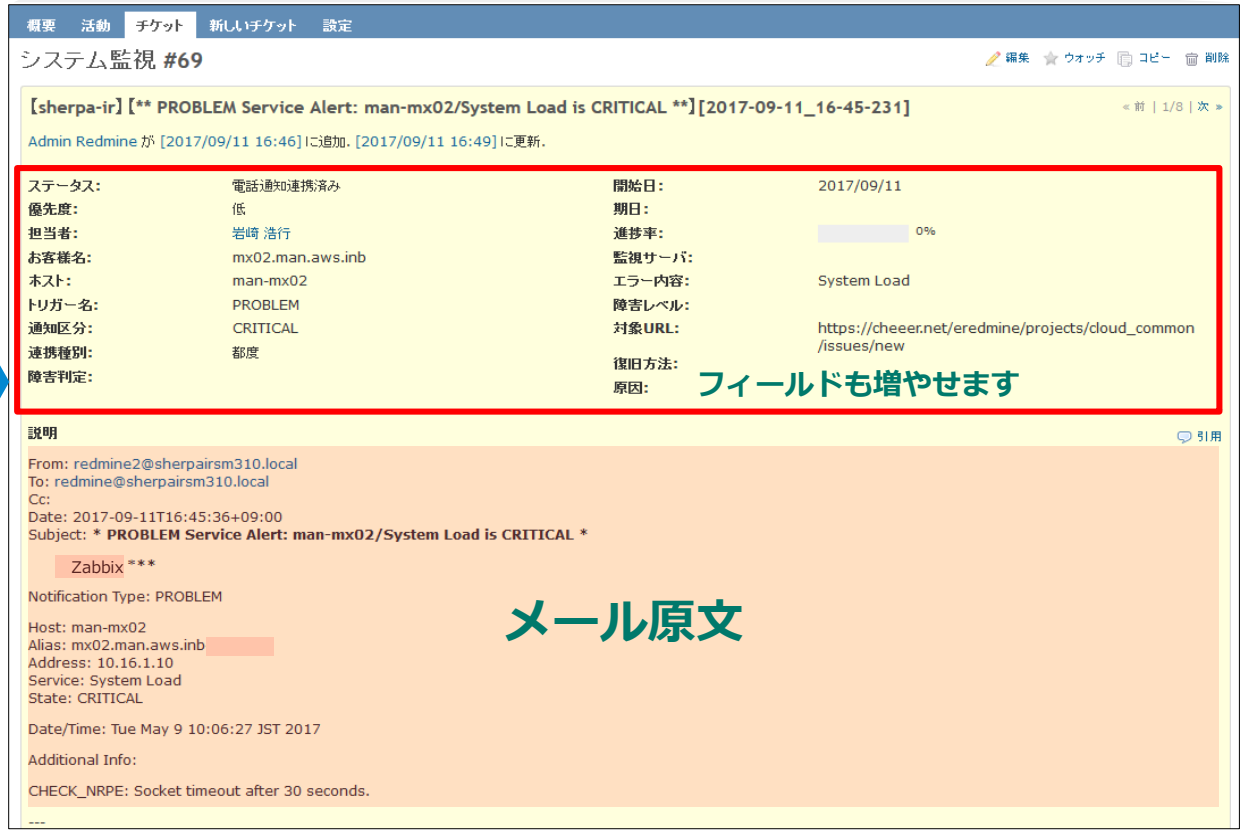
✓全ての通知を自動取込み	（対応漏れが無くなる）
✓必要な項目を自動転記	（起票ミス／記載漏れ無し）
✓該当担当者通知	（譲り合っての対応遅延防止）
✓全ての進捗状況の把握	（運用品質の向上）

SHERPA-SM　アラートメール自動取込み機能

【Zabbixからの通知メールサンプル】

名前：アラートメール送信
デフォルトの件名：【障害】{TRIGGER.NAME}:
{ITEM.LASTVALUE}: zabbix
デフォルトのメッセージ：
Original event ID: {EVENT.ID}
障害発生時刻：{DATE} {TIME}
ホスト名：{HOST.HOST}
IPアドレス：{HOST.IP}
設置場所：{INVENTORY.LOCATION}
深刻度：{TRIGGER.SEVERITY}
障害内容：{TRIGGER.NAME}
最新値：{ITEM.LASTVALUE}

必要な情報を自動取り込み



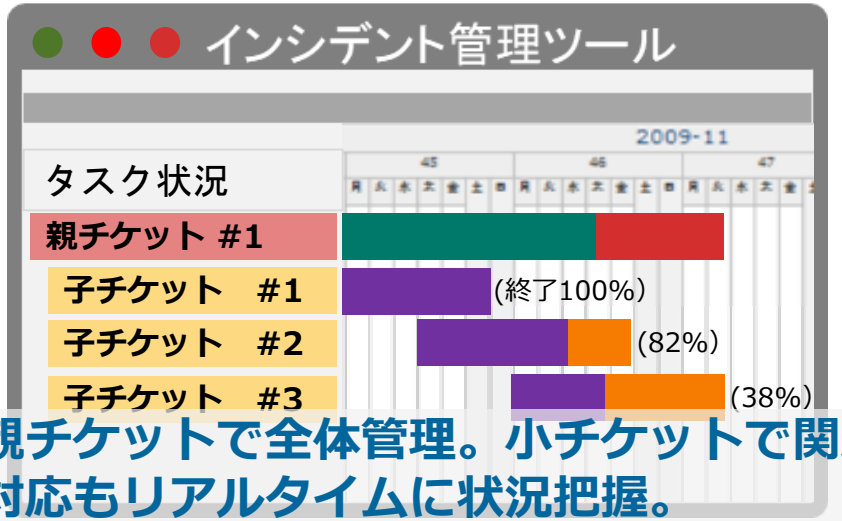
記入漏れや情報不足などのミスを防止

SHERPA-SM　その他機能

マイページ

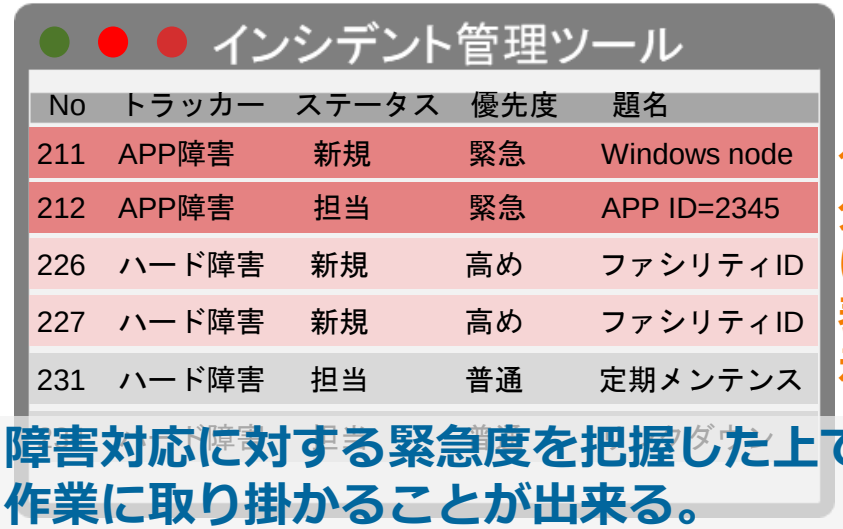
自分の担当分が直ぐにわかり
対応漏れが無くなる。

ガントチャート



親チケットで全体管理。小チケットで関連
対応もリアルタイムに状況把握。

優先度表示



色分け表示

障害対応に対する緊急度を把握した上で
作業に取り掛かることが出来る。

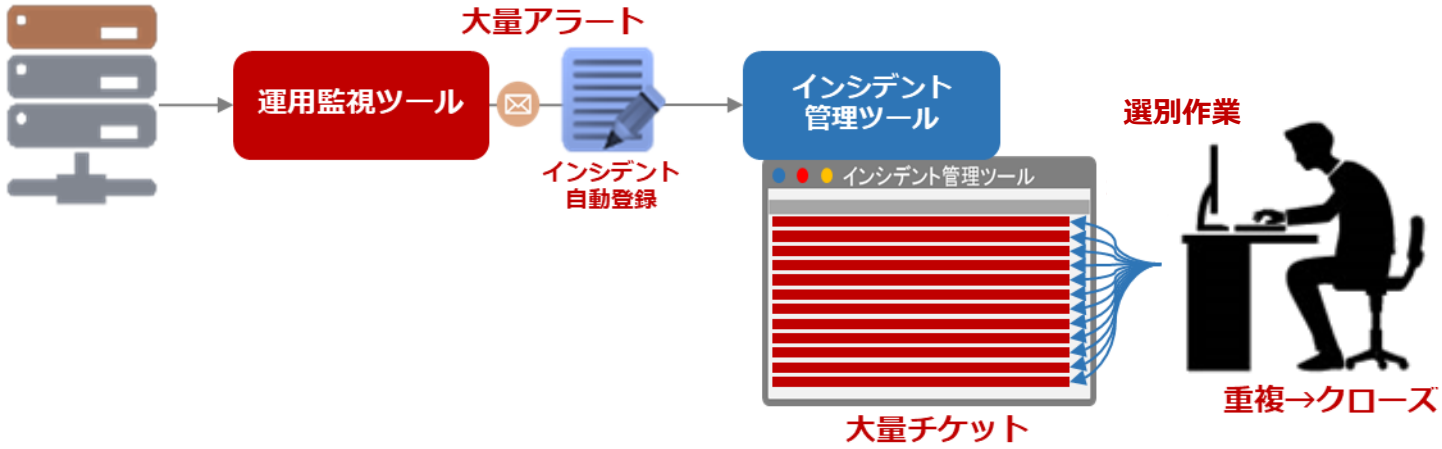
対応履歴の検索

対応履歴を共有することで、障害復旧時間
を短縮や対応品質の均一化が出来る

公開

監視ツールとインシデント管理を自動連携

監視ツールとインシデント管理を自動連携するとこのような状況になることがあります。



✓同一原因による沢山のアラートが大量のインシデントとして登録される。

✓登録された不要なインシデントを確認後チケットクロース処理を行う。

✓担当外の障害にも拘らずアラートが飛んでくる。

オペレータの作業増大

人手による運用１次オペレーション作業の増加は、障害復旧作業開始までの遅延や運用１次オペレータの作業ミスを誘発します。

公開

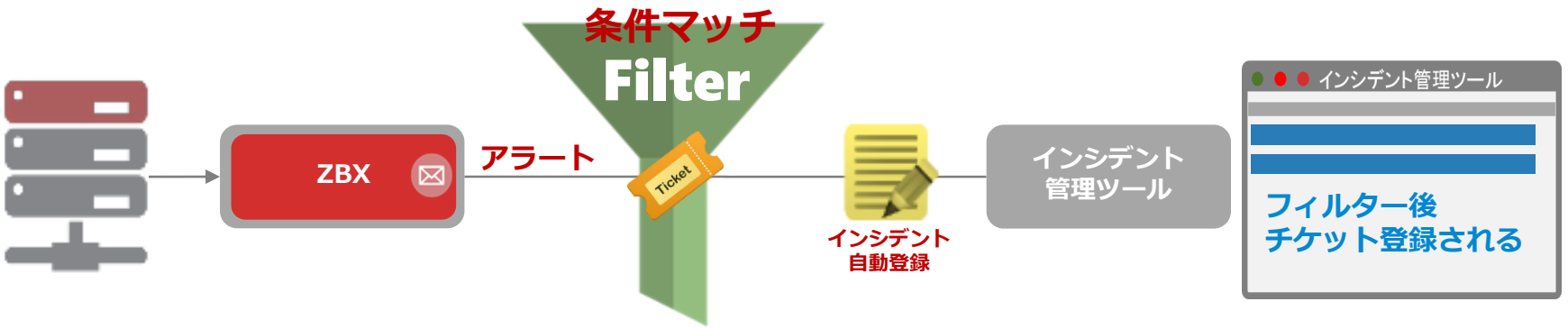
インシデント管理をうまく回すには・・・・

インシデント管理にうまく自動連係するには・・・・・

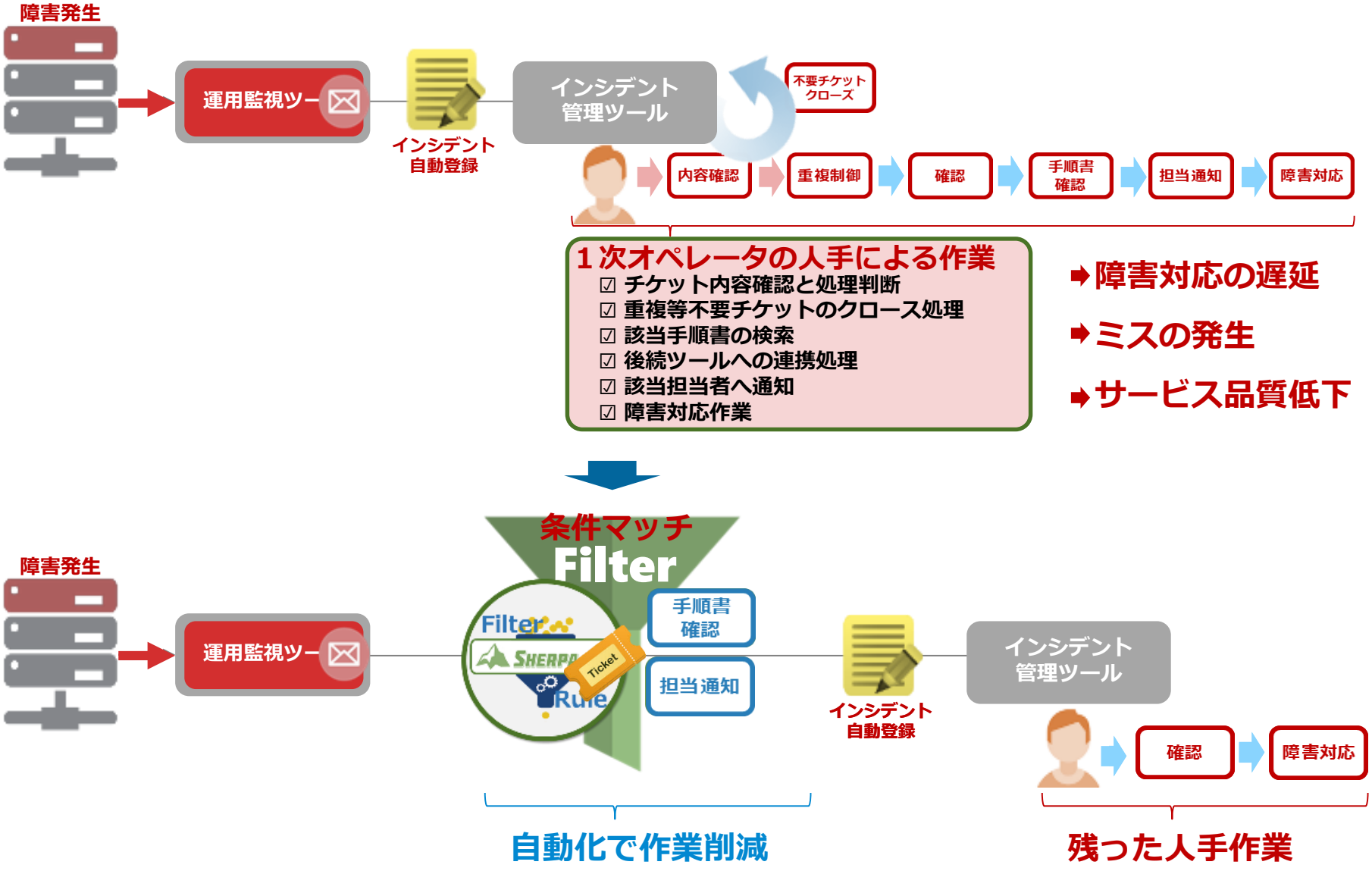
- ✓ インシデント登録は必要モノ以外は登録しない。
- ✓ インシデントはオペレータによる処理作業が必要なもの絞る。

具体的にはどうすれば良いのか？？？？？？？

- ✓ インシデント管理に登録する前に不要なものはフィルタすれば良い



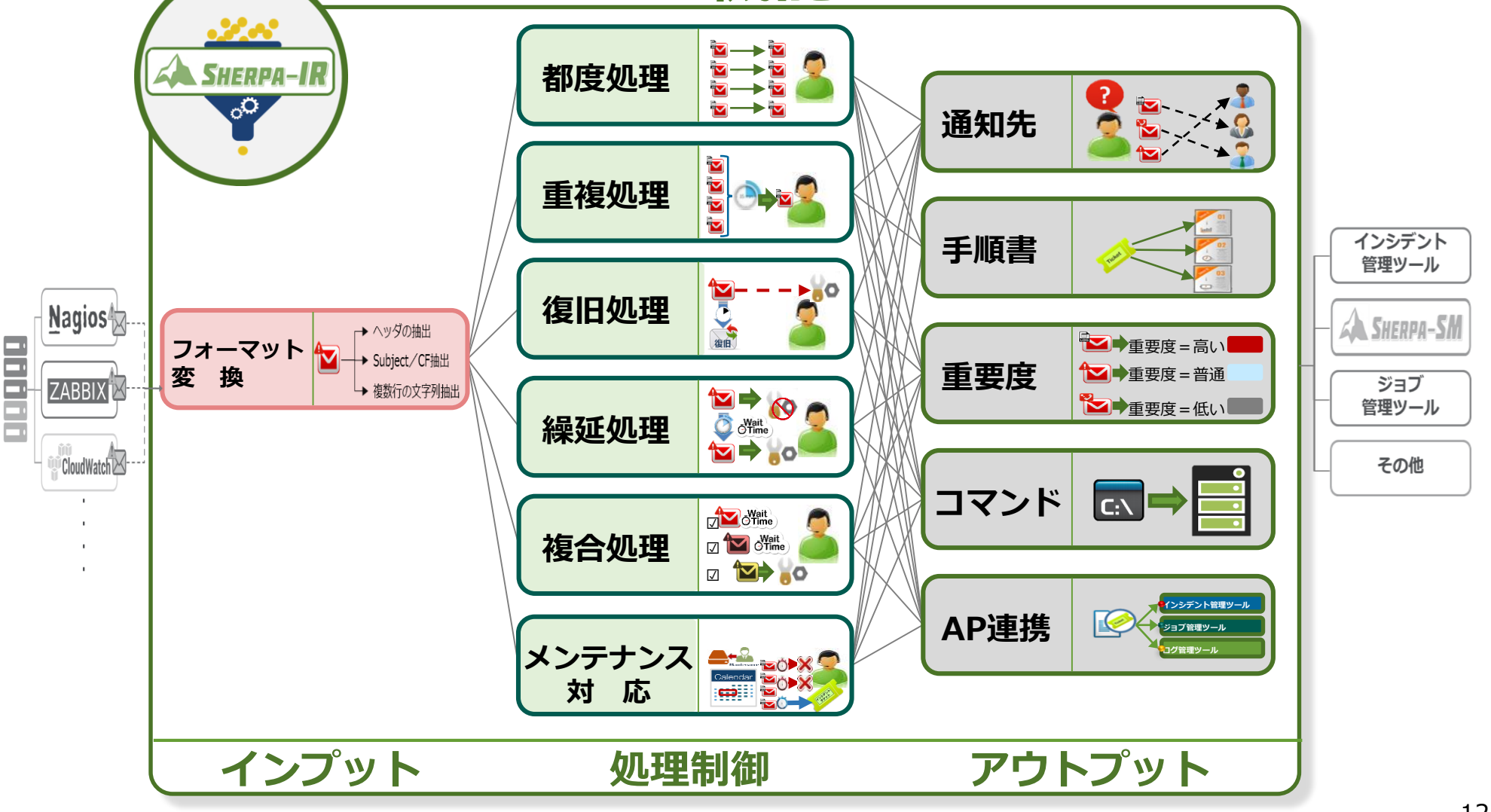
SHERPA-IRは1次オペレータ作業の自動化を支援



公開

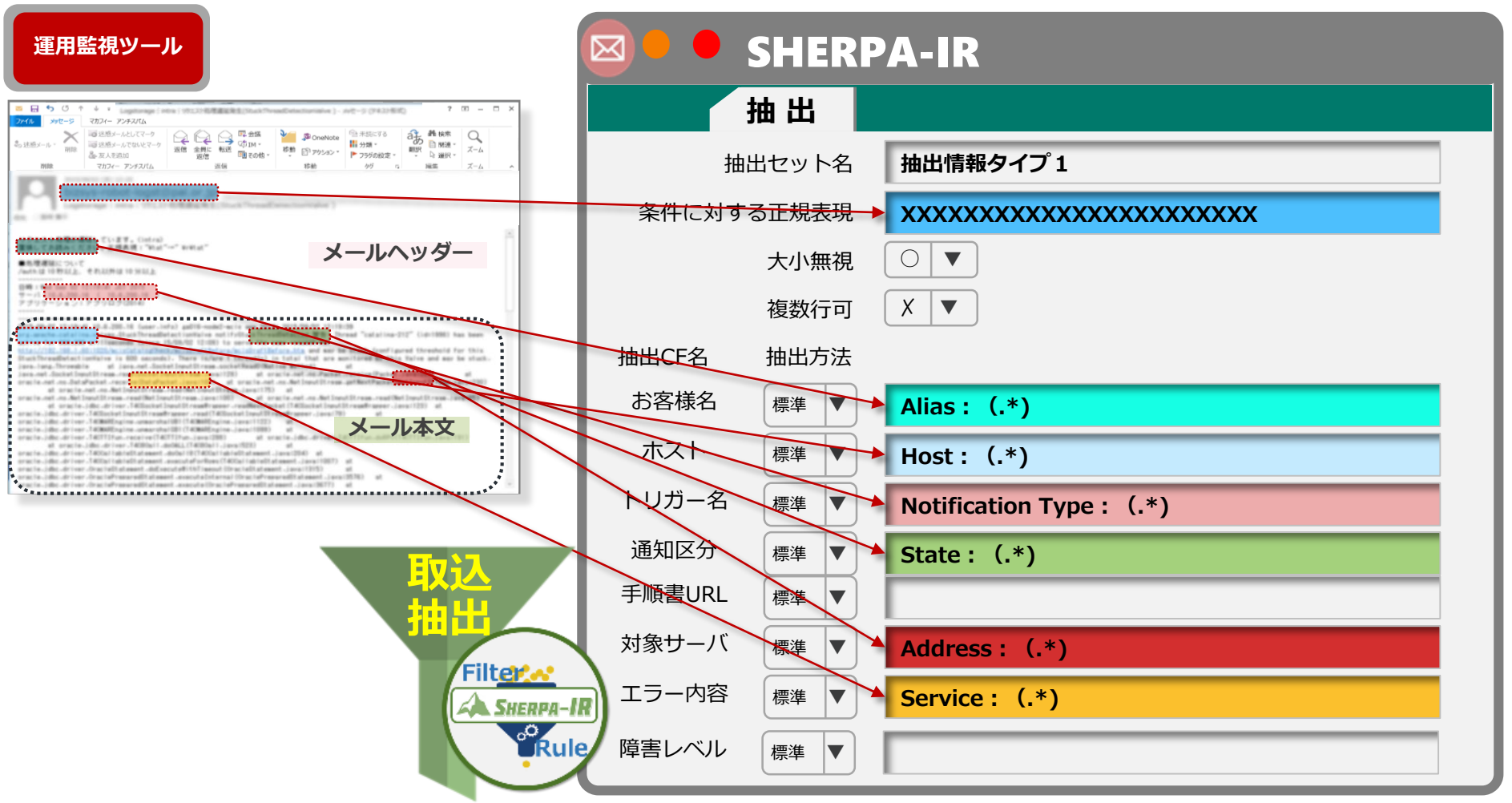
イベント制御ツール　＝　SHERPA－IR

SHERPA-IR機能



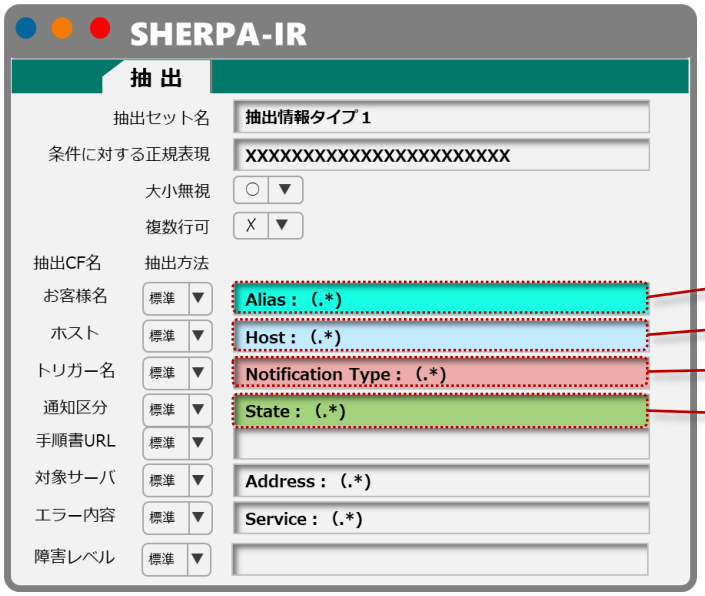
アラート取込み（フォーマット変換）／　抽出処理

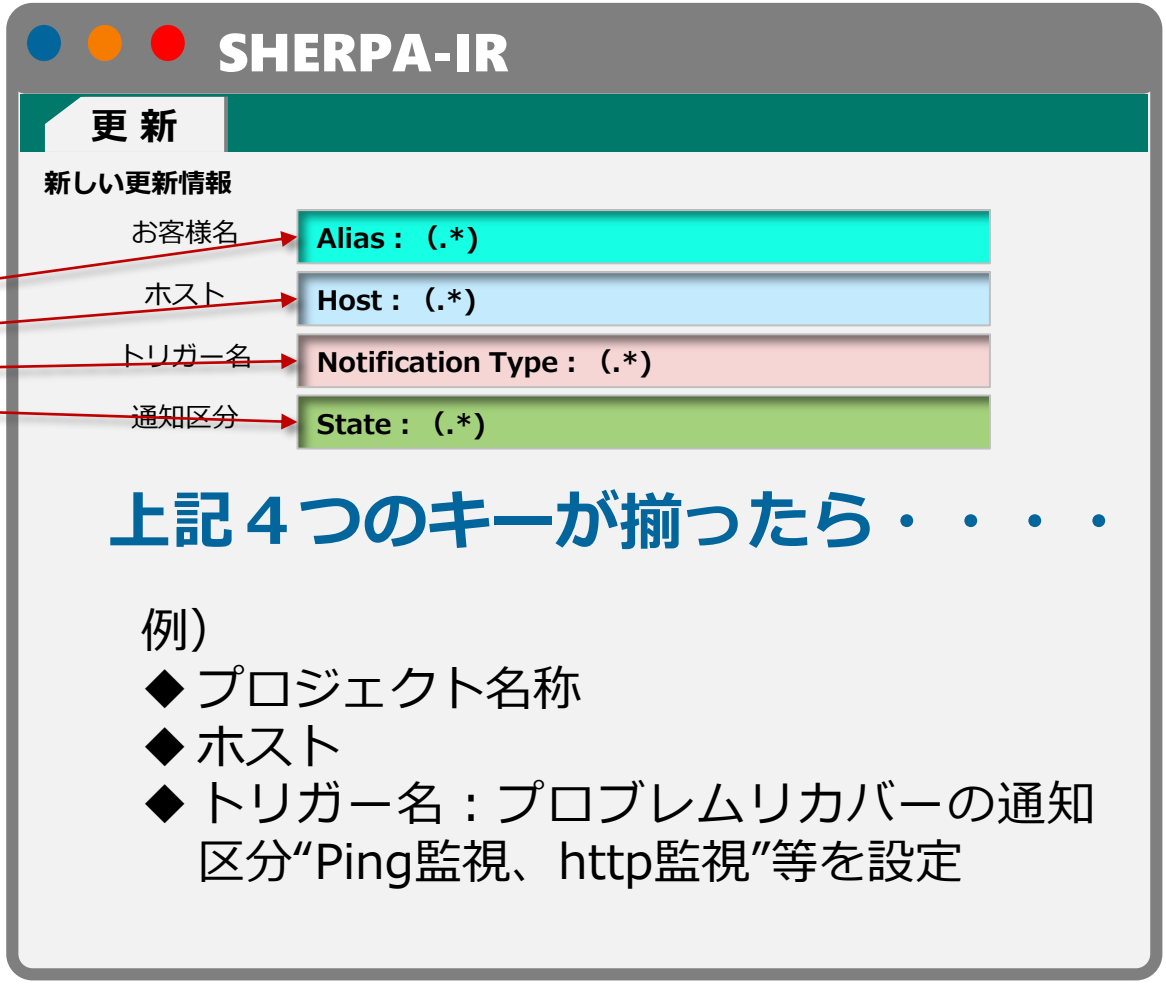
フィールドに設定したい値を入力します。今回の例では、メールテンプレートの内容をフィールドに設定し、メールの件名からパターンを洗い出し正規表現で設定。



設定：更新処理　どのようなアラートが来たら？

アラート内容を一意に判定する為に、事前に設定した“４つのキー項目”文字列や＊等を設定します。



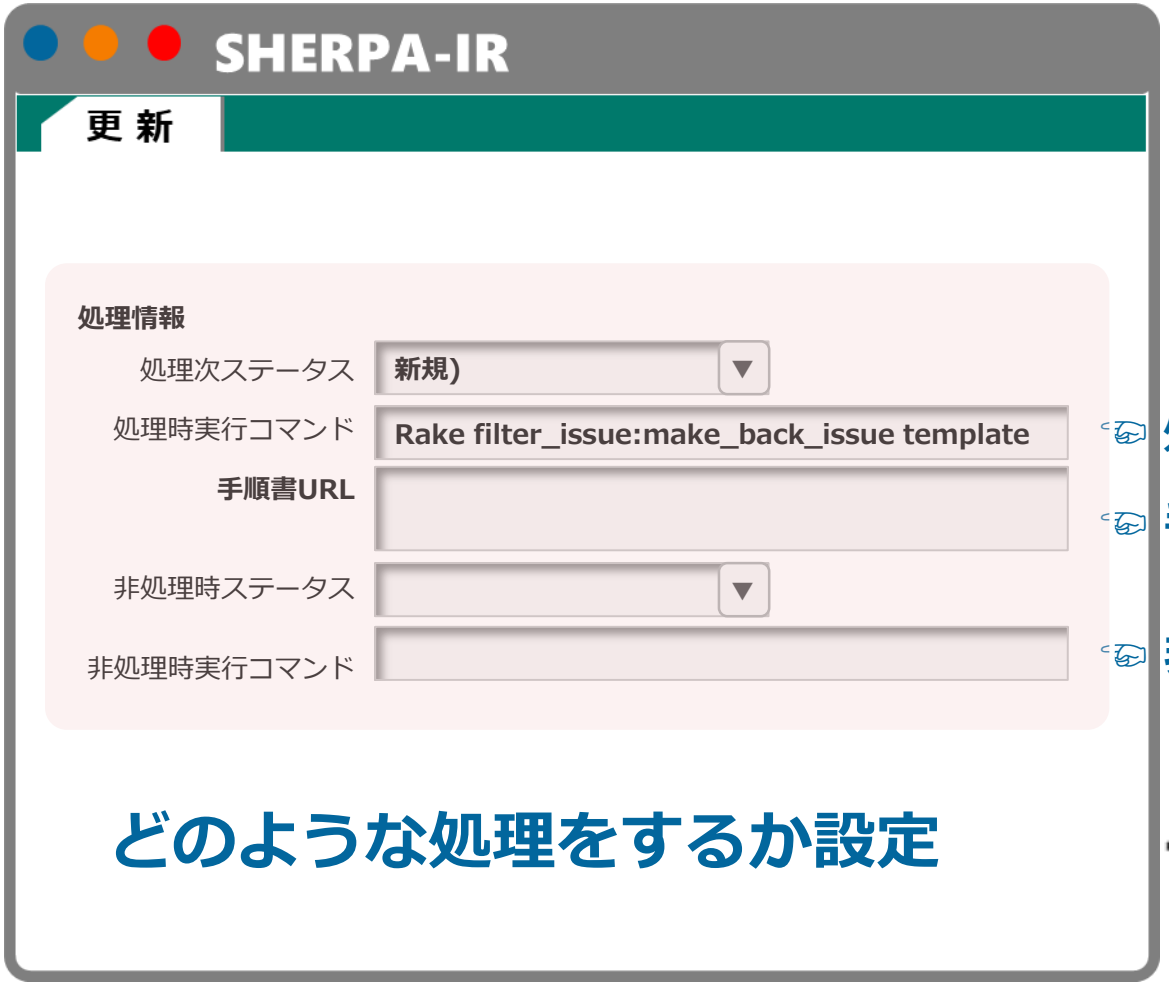


上記４つのキーが揃ったら・・・

例）
- ◆プロジェクト名称
- ◆ホスト
- ◆トリガー名：プロブレムリカバーの通知区分“Ping監視、http監視”等を設定

設定：更新情報設定　どのような処理をさせるか？

処理したい作業を記述します。
コマンド登録（複数可）や、付加情報として手順書のURLや通知先を登録。



処理したいコマンド登録（複数可）

手順書URL情報を通知

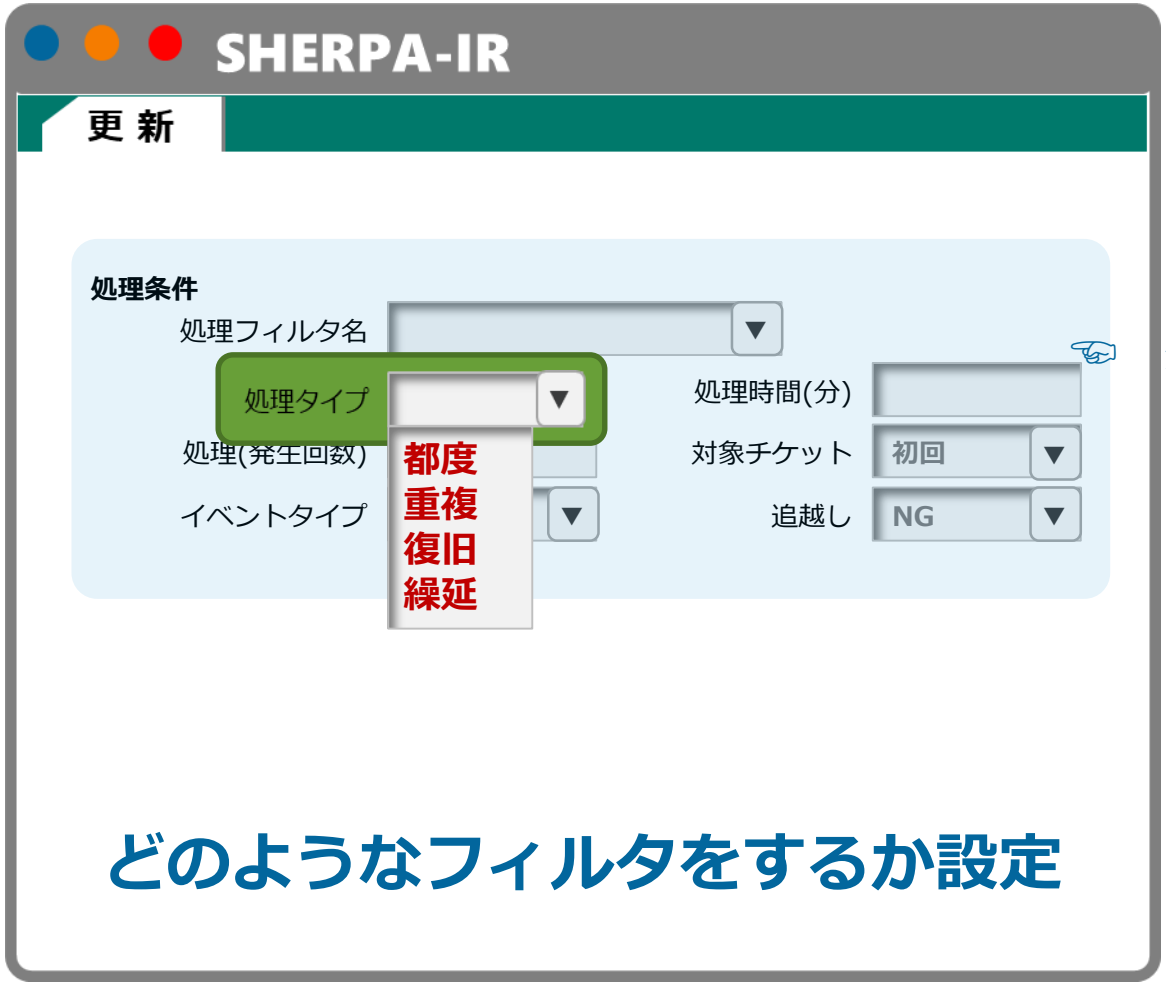
非処理時のコマンド登録（複数可）

設定作業

手順書はSHERPA-SMのWiki・文書にUPするとURLが表示され利用出来ます

設定：更新条件設定　どのようなフィルタをするか？

何にどんな処理をさせるのかの設定は終わったが、同一の複数アラートに対して処理タイプを選び集約させます。



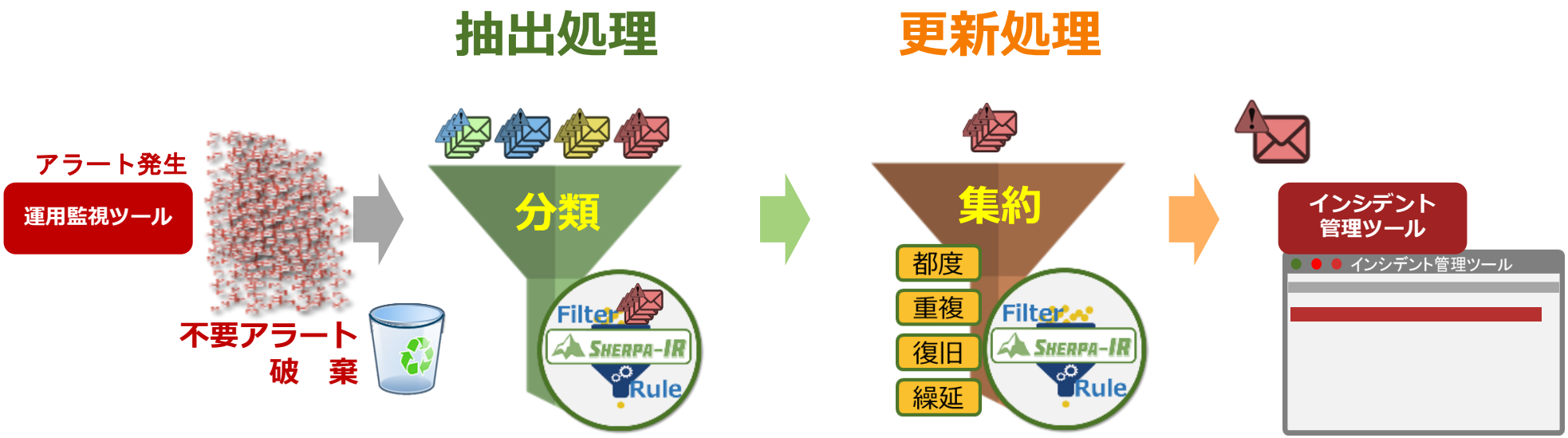
処理タイプ（フィルター）を設定

- **都度：付加情報を付けて都度通知**
- **重複：指定時間帯の同一アラート抑制**
- **復旧：復旧報によるアラート抑制**
- **繰延：期間繰延アラート抑制**

設定作業

SHERPA-IRの処理の流れとアラートフィルターの様子

以下の様な流れで、複数のアラートをインシデントとして登録するチケットに集約していきます。

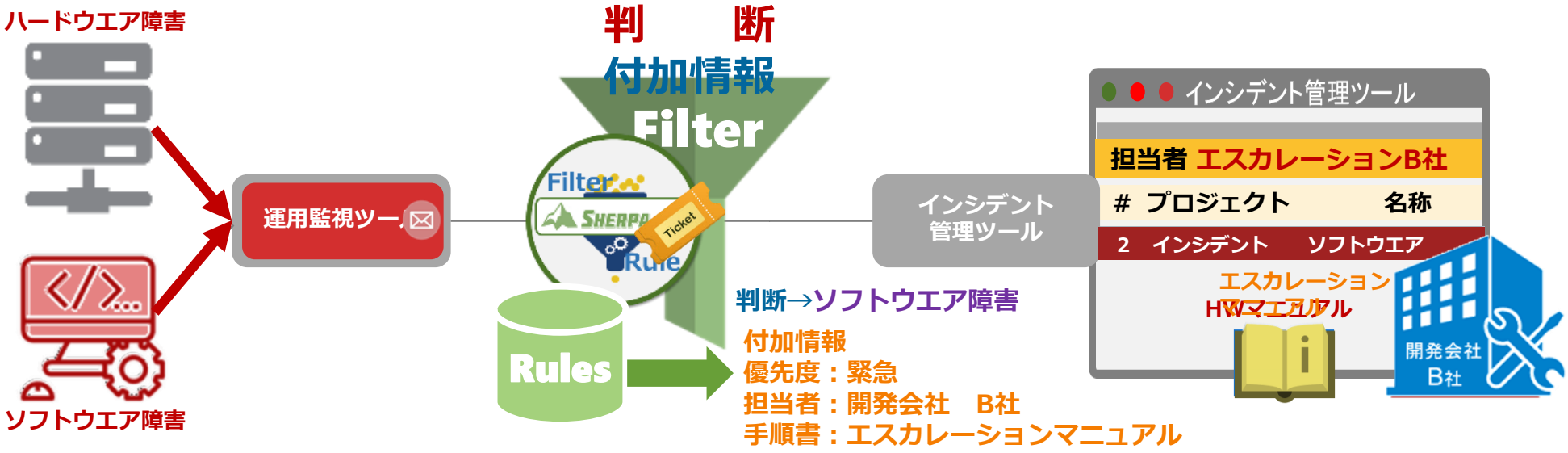


アラートをキー情報で分別
※通知が重複しているかは見ていない

４つの処理タイプを使って
チケットを集約し登録します。

SHERPA-IRの機能：追加情報登録

アラートに対する情報を追加してインシデント登録が出来ます。



付加情報によるメリット

1．手順書情報：インシデントに対応する手順書URLが付加されるので直ぐに障害対応へ

2．担当者情報：障害の担当者やエスカレーション先に自動通知。障害対応見落とし削減

SHERPA-IRの機能：重複処理（フィルタリング）

同一のアラートが指定した時間帯に 指定回数通知された場合に、インシデント登録を行います。

重複処理対応メリット

1．アラート内容確認から解放

2．重要アラート見落とし削減

3．ミスの軽減

4．サービスレベルの均一化

SHERPA-IRの機能：繰延処理

既に障害対応作業に取掛っていても、障害復旧していなければ、設定時間をすぎると新たにインシデントが作成されてしまいす。（重複処理）
繰延処理は、指定した時間内に同一のアラートが通知された場合、指定時間のタイマーをクリアー（繰延）し、制御を継続することが出来ます。

繰延処理対応メリット

1．作業時間を気にすることなく、障害対応に専念できる

SHERPA-IRの機能：復旧処理

復旧処理は、対象機器からの“障害報”と“復旧報”を考慮する処理タイプです。
LinkDown/LinkUP等ネットワーク機器で、“障害報”が通知された場合、一定時間”対”となる”復旧報”を静観する場合があります。復旧処理では“障害報”が来ても直ぐにチケット作成指示を出さず、一定時間”復旧報”を持ち、通知されれば障害報を無視し、通知が無ければチケット作成指示を実施します。

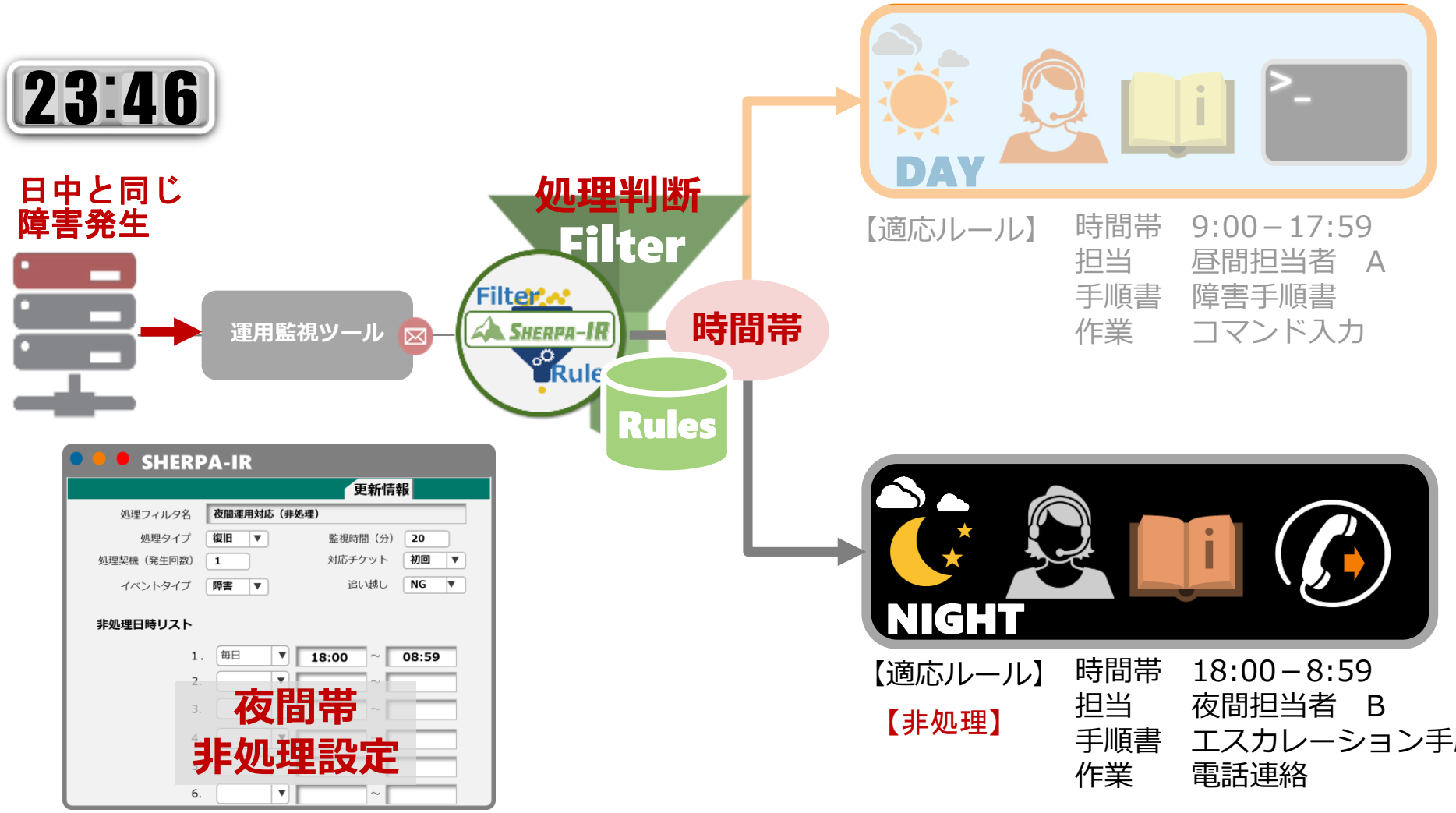
繰延処理対応メリット

1. “対”となるアラート待ちからの解放
2. 不要チケットの消込作業削減

公開

SHERPA-IRの機能：非処理

同じアラートでも、曜日や時間帯を考慮して通常の処理をしない“非処理”



SHERPA-IRの機能：メンテナンス

メンテナンス時のアラート制御は、“指定機器”及び“指定時間帯” を非処理機能を利用して行います。指定時間帯のメンテナンス機器からのアラートは無視されます。　メンテナンス時間帯でも、指定されていない機器からのアラートは、通常の制御として処理されます。

メンテンンス時処理メリット

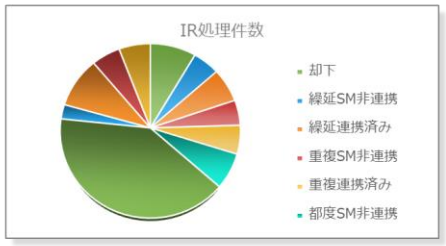
1. メンテナンス作業中の作業サーバ停止による大量不要アラートからの解放
2. 不要チケットの消込削減

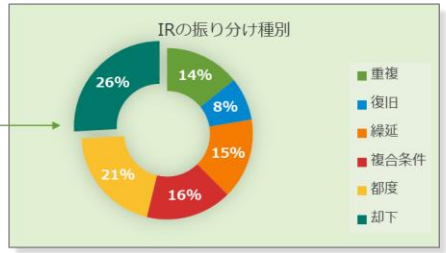
公開

SHERPA-IR機能：レポート

cybertrust

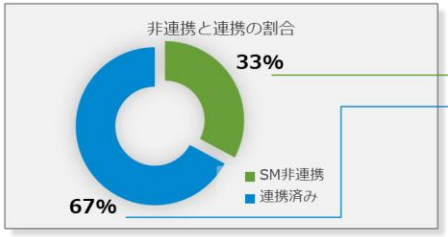
単月の登録内容

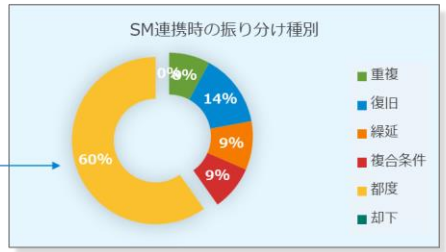




単月のIR処理数とSMへの連携数

(下のグラフは3割ほどIRで処理)

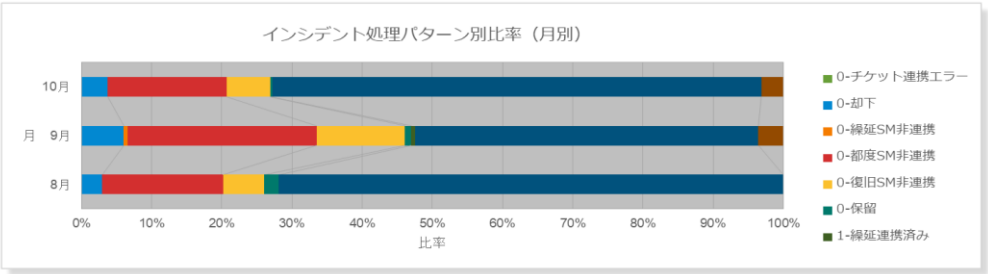




※ 処理タイプ「都度」が良く使われている。
※ 連携すべきインシデント化の精査が必要。

3か月のIRで利用している処理タイプ別割合

サマリ	列ラベル									
行ラベル	0-チケット連携エラー	0-却下	0-繰延SM非連携	0-都度SM非連携	0-復旧SM非連携	0-保留	1-繰延連携済み	1-都度連携済み	1-復旧連携済み	総計
8月		7		41	14	5		171		238
9月		62	6	277	130	9	6	503	37	1030
10月	1	58		268	98	4		1100	49	1578
総計	1	127	6	586	242	18	6	1774	86	2846



SHERPA-IR Reporterを利用して、削減効果報告や運用改善提案へ

処理タイプと処理件数の分析で運用改善の仮説検証へ展開

SHERPA-IR導入の進め方

お客様の作業条件を確認し、SHERPA-IRのルールに落とし込んできます。

- ■重複　->　“tx”を含むホスト名の場合、重複制御
- ■都度　->　”app”を含むホスト名の場合、都度電話連絡
- ■復旧　->　“spice”を含むホスト名のHTTPで20分以内にリカバリを検知した場合、電話通知不要

重　複

件名：** PROBLEM Service Alert: tx-ap01/Application Log - API is CRITICAL **

***** Nagios *****

Notification Type: PROBLEM

Host: tx-ap01
Alias: ap01.tx.aws.inb-xxxxx .jp
Address: 10.16.20.10
Service: Application Log - API
State: CRITICAL

Date/Time: Mon Nov 21 15:23:01 JST 2016

都　度

件名：** PROBLEM Service Alert: cmf-app01/Application Log is CRITICAL **

Host: cmf-app01
Alias: app01.cmf.aws.inb-xxxxx .jp
Address: 10.16.46.10
Service: Application Log
State: CRITICAL

Date/Time: Sat Jul 22 11:57:44 JST 2017

Additional Info:

CRITICAL - (2 errors) - 22-Jul-2017 11:55:39.807 SEVERE [ajp-nio-8009-exec-1353] org.apache.catalina.core.StandardHostValve.custom Exception Processing ErrorPage[exceptionType=java.lang.Exception, location=/WEB-INF/views/common/error/unhandledSystemError.html] ...

復　旧

件名：** PROBLEM Service Alert: [xxxxx]spice-api/HTTP is CRITICAL **

***** Nagios *****

Notification Type: PROBLEM

Host: [xxxxx]spice-api
Alias: [xxxxx]spice-api
Address: spice-native-api.xxxxx .jp
Service: HTTP
State: CRITICAL

Date/Time: Sat Jul 22 12:08:23 JST 2017

相対するメール

件名：** RECOVERY Service Alert: [xxxxx spice-api/HTTP is OK **

***** Nagios *****

Notification Type: RECOVERY

Host: [xxxxx]spice-api
Alias: [xxxxx]spice-api
Address: spice-native-api.xxxxx .jp
Service: HTTP
State: OK

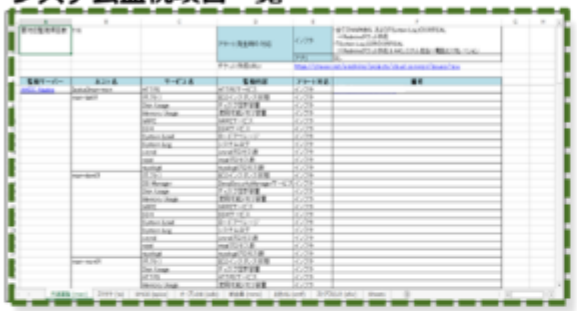
Date/Time: Sat Jul 22 12:13:13 JST 2017

SHERPA-IR導入の進め方

cybertrust

どのようなアラートが来たらどの処理（フィルタ含む）をするかを整理し、SHERPA-IRのルールに設定していきます。

システム監視項目一覧



アラートメールサンプル　①、②、③、④

フィルタールール

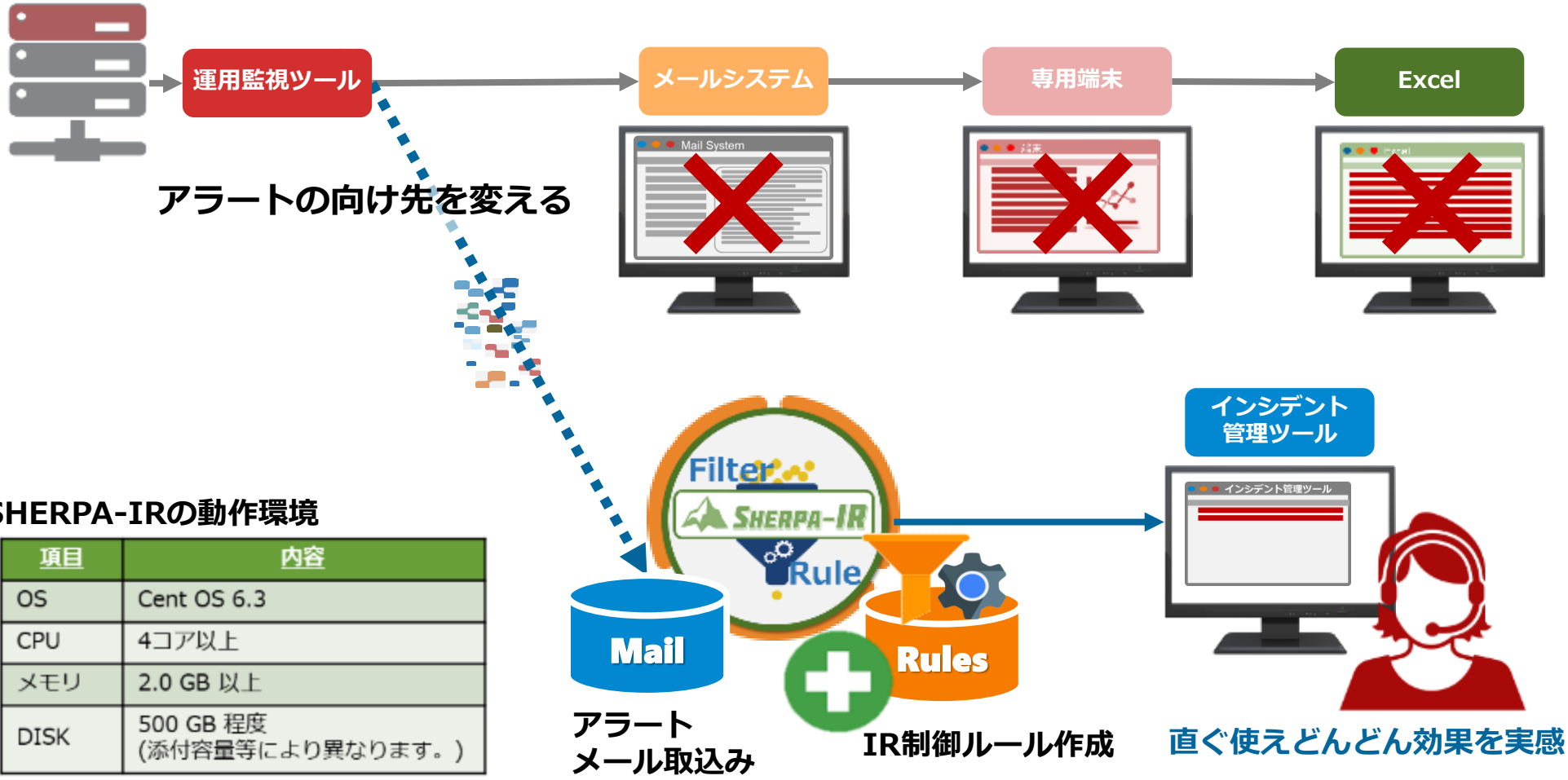
ホスト名	サービス名	監視内容	アラート対応	アラート発生時の対応	サンプル種別	処理タイプ
cmf-app01	Application Log	アプリケーションログ	アプリ	チケット作成	サンプル① チケット作成のみ	都度
tx-dbr01	MySQL	MySQLサービス	インフラ			
man-mx02	System Load	ロードアベレージ	インフラ	チケット作成 & AWシステム担当へ電話エスカレーション	サンプル② 要電話通知	都度 (電話通知)
spice-dbm01	Disk Usage	ディスク空き容量	インフラ	チケット作成 & AWシステム担当へ電話エスカレーション		
tx-ap	Application Log - API	アプリケーションログ	アプリ	チケット作成 更に30分で3回以上発生した場合のみアプリ担当へ電話連絡	サンプル③ 要電話通知(重複)	重複
spice-api	HTTP	HTTPサービス	インフラ	お客様にも電話連絡する。 20分でリカバリを検知した場合 システム担当者含め電話連絡不要		復旧
spice-push01	Memory Usage	使用可能メモリ容量	インフラ	チケット作成	サンプル④ チケット作成のみ(復旧)	重複+復旧

SHERPA-IR

Rule

SHERPA-IRの配置

SHERPA-IRの導入は、大きなシステム変更をする必要はありません。

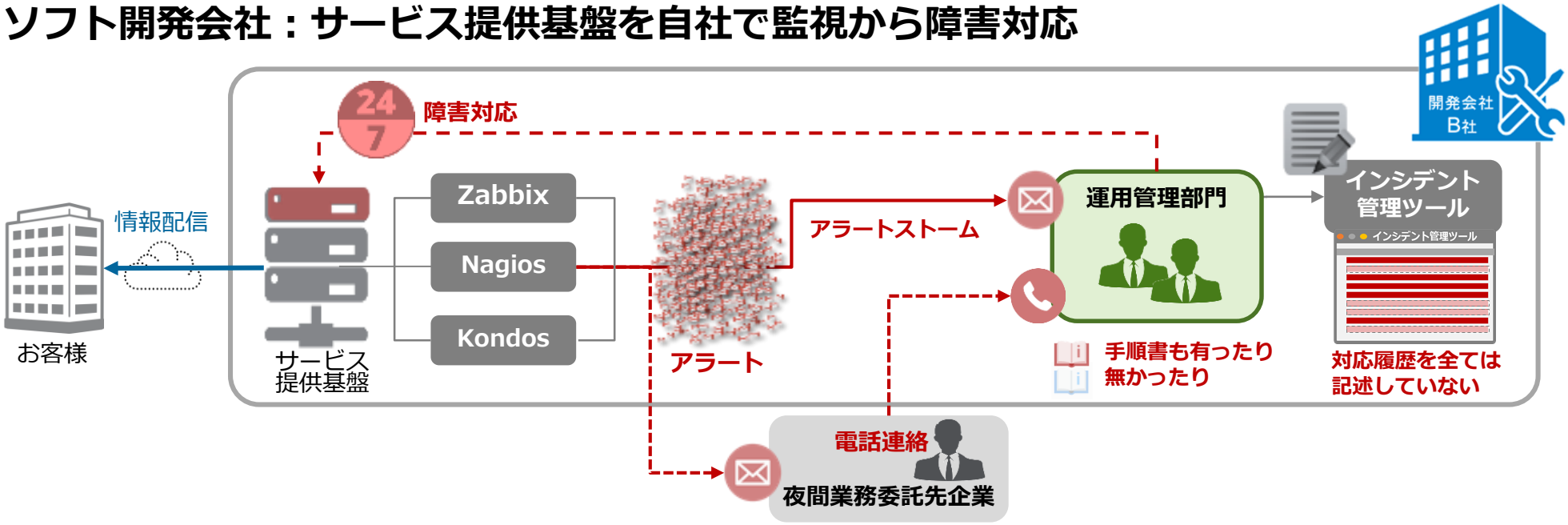


SHERPA-IRの動作環境

項目	内容
OS	Cent OS 6.3
CPU	4コア以上
メモリ	2.0 GB 以上
DISK	500 GB 程度 (添付容量等により異なります。)

導入事例

ソフト開発会社：サービス提供基盤を自社で監視から障害対応



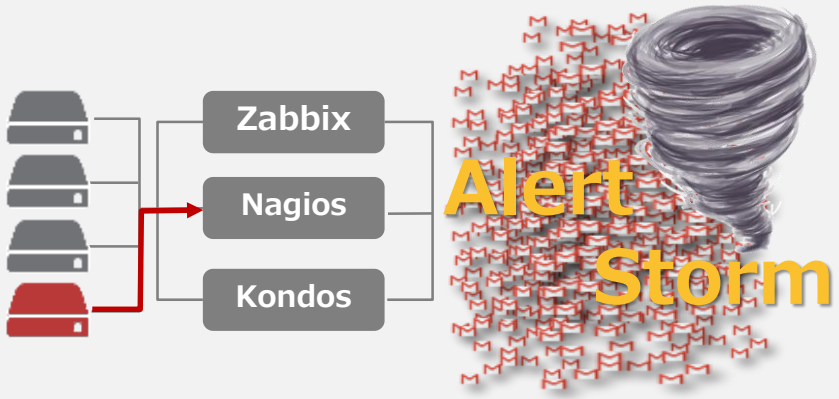
目標：コストを抑えて運用アウトソースしたい。

課題

① アラートストームを含め大量に発生する
② 障害アラート内容を確認し対応するか否かを人が判断している
③ 匠運用に頼り障害対応手順書が整備されていない
④ 障害対応履歴も手入力で全ては登録していない
⑤ 24時間対応が出来ていない

現状環境条件ではコストが高くなり、障害対応まで含めた作業を依頼することが出来ない。

導入事例：チューニング

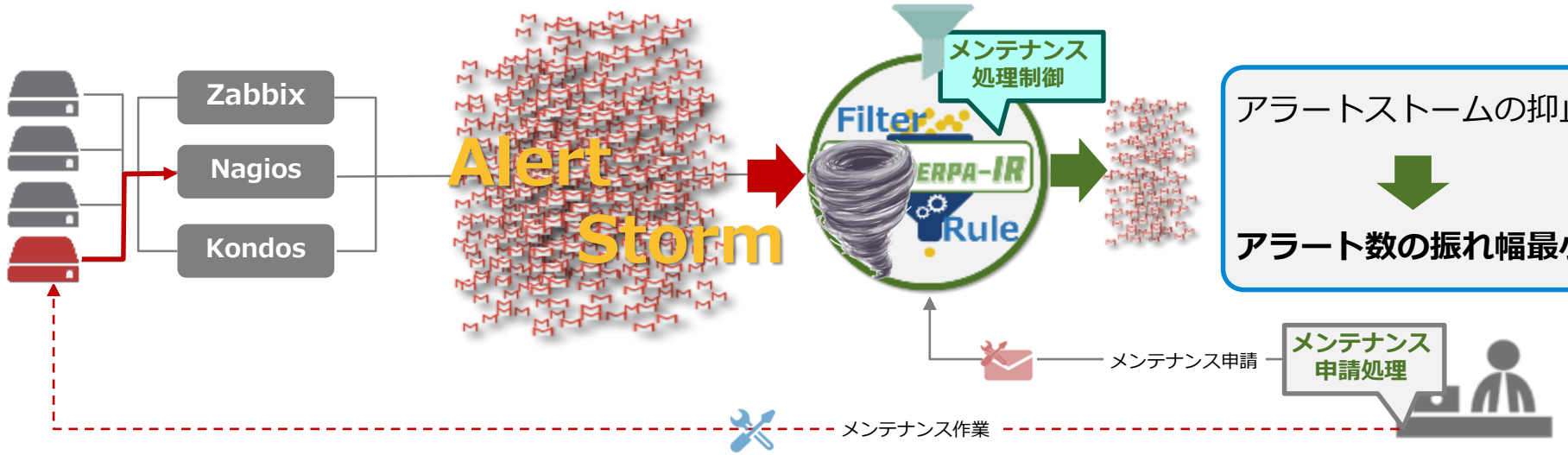


大量アラートの原因は・・・

①申請なしのメンテナンス作業によるアラート

②同一障害のアラートが複数通知される

改善：メンテナンス申請関連改善によるアラートストームの抑止



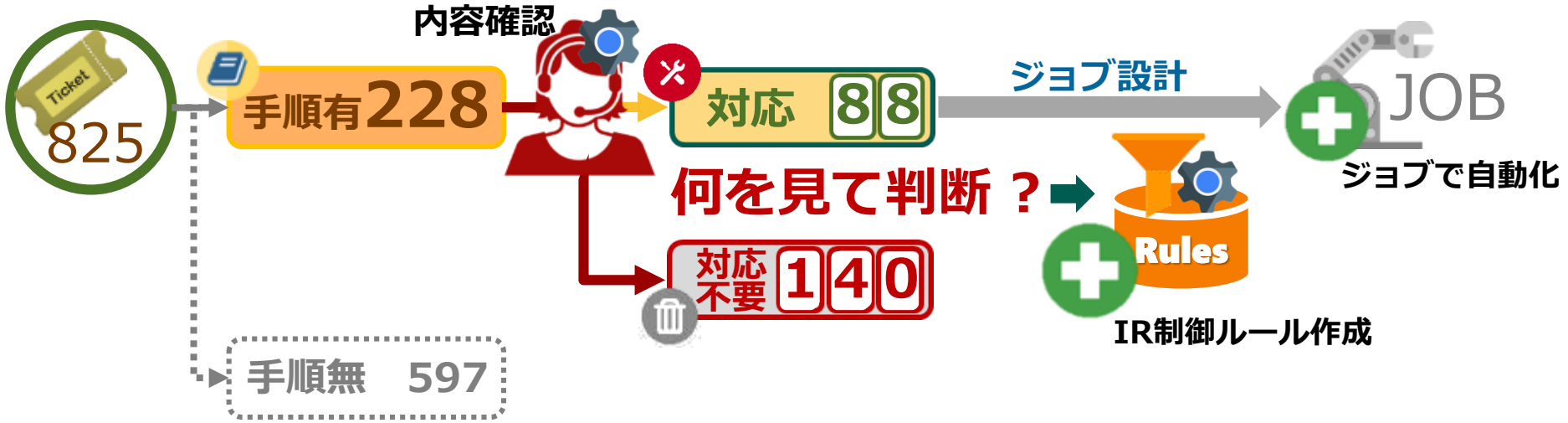
公開

導入事例：先ずはIRを通したインシデント登録フロー作成

先ずはじめは処理タイプ“都度”を設定し、SHERPA-IRを利用するルートを設定し利用開始。
（明確に不要なアラート以外は都度登録となり、重複チケットのクローズ処理が発生している。）

導入事例：定期チューニング

- ☑ 手順有りの通知数がが、限りなく対応件数と近くなるようにIRルールを見直し
- ☑ 人手による障害対応作業をジョブにて自動化



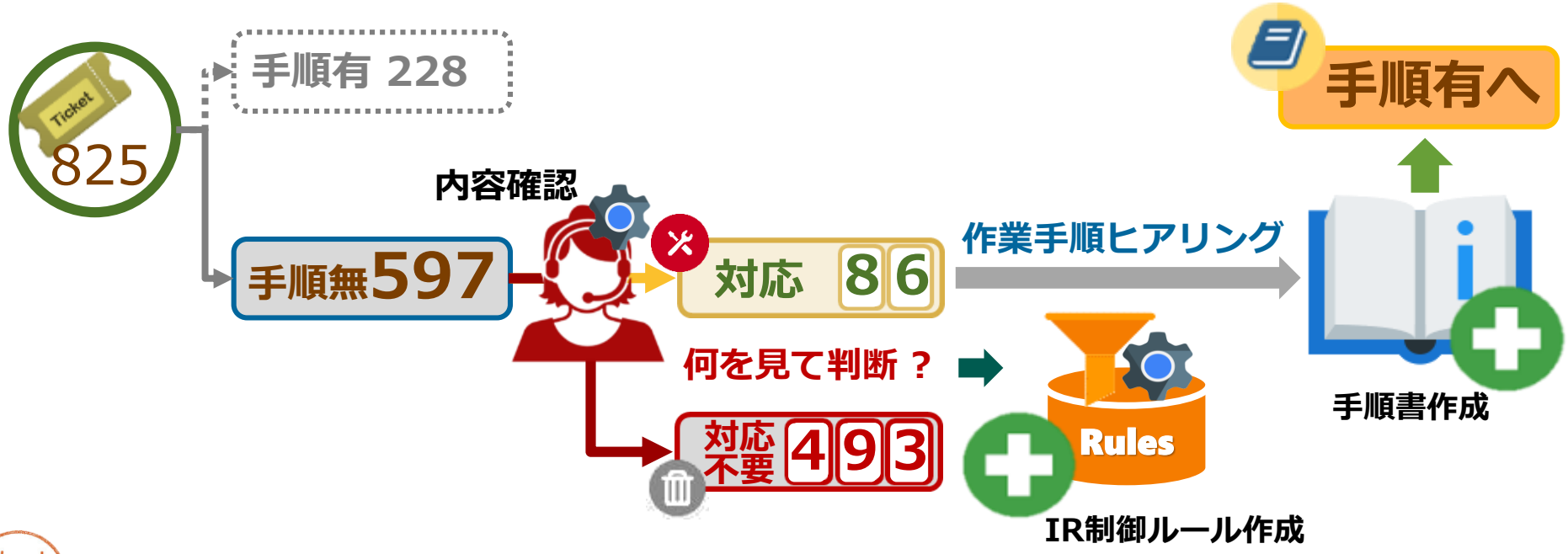
Check Point

対応作業の内容からジョブ管理ツールで自動化できないかの検討。

通知内容より“対応”or“不要”の判断時間の短縮

導入事例：定期チューニング

- ☑ 手順無しで且つ障害対応したインシデントに対して新たに作業手順書を作成
- ☑ 手順無し通知数が、限りなく対応件数と近くなるようにIRルールを見直し



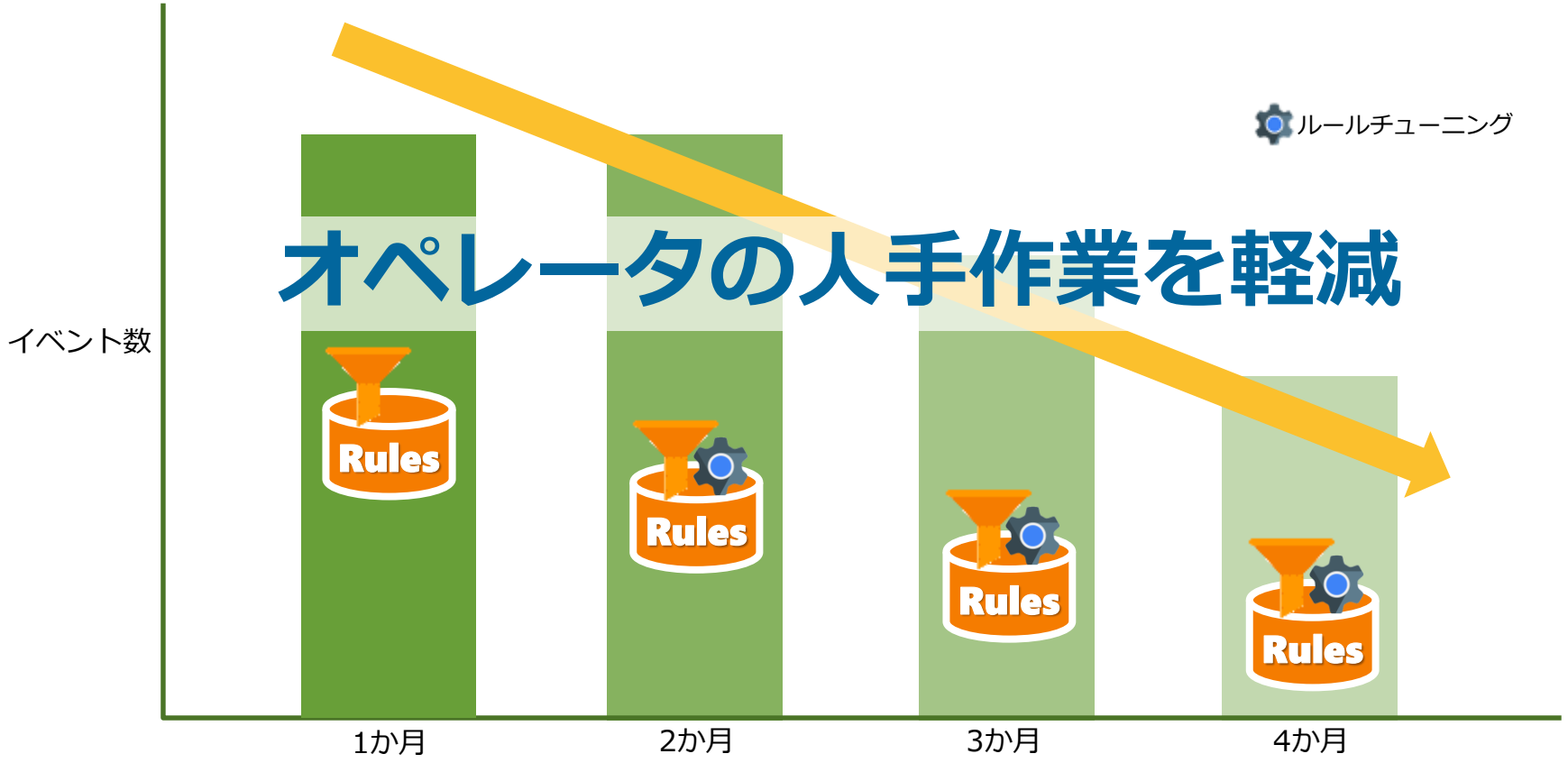
Check Point

手順書を作成し紐付ける事により、アウトソースへ依頼できる対象件数の拡大。

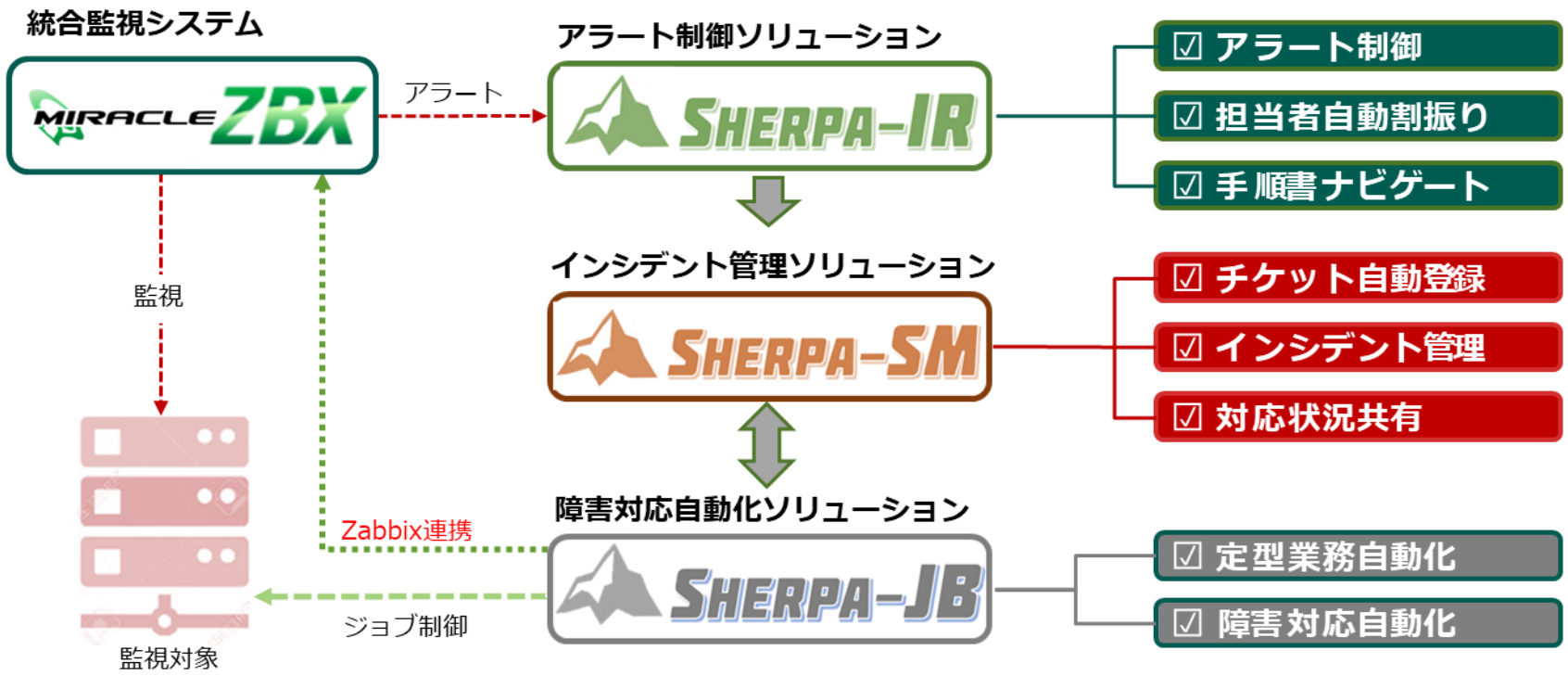
通知内容より“対応”or“不要”の判断時間の短縮

導入事例：定期チューニング

イベント内容を解析しルールを更新する定期チューニングを繰り返し行うことで、
アラート件数の削減を実現し、リスクの高い重要なインシデントに絞り込むみ
オペレータの人手作業を軽減できます。



ご提供ソリューションMAP



出来るところから運用業務の自動化を始めましょう！

公開

SHERPA-IR導入アセスメント

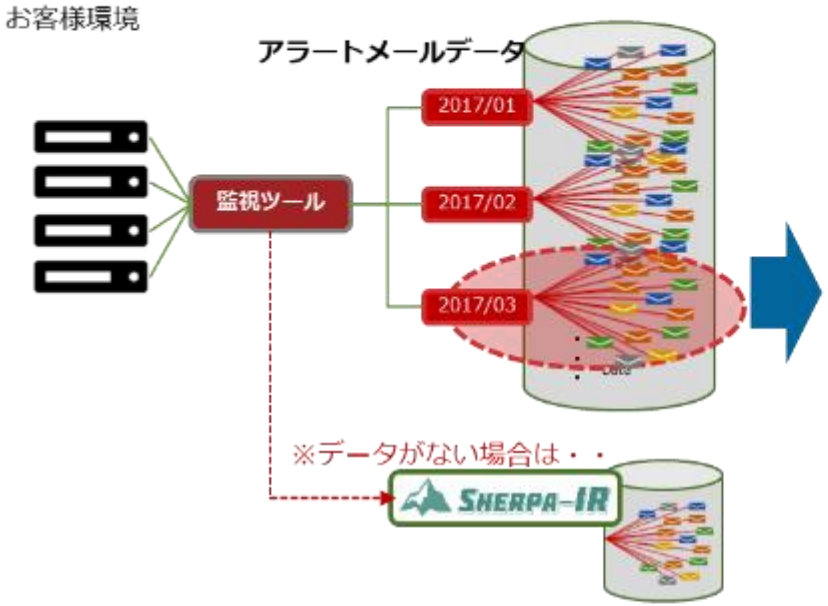
色々と良さそうな事聞いたけど・・・・・

うちの運用環境で使えるのかなぁ？？・・・・・

SHERPA-IR導入アセスメント

SHERPA-IR導入アセスメント

実際のお客様のアラートメールデータを分析して、SHERPA-IR導入の効果がありそうかの予測



区分	サンプリング	分類	ルールパターン	削減効率
作業	一定期間メールインシデントをもらう又は、自社SHERPA-IRに飛ばしてインシデントを蓄積	障害報および復旧報が発生するインシデントを特定	定期的に発生しているインシデントを見つけ、重複等ルールが使えそうか予測	IR導入による削減予想レポート また、障害対応の自動化による削減予測
アウトプット		インシデント分類	IRルール適応分類	導入効果予測

SHERPA-IR導入アセスメントレポート

利用目的

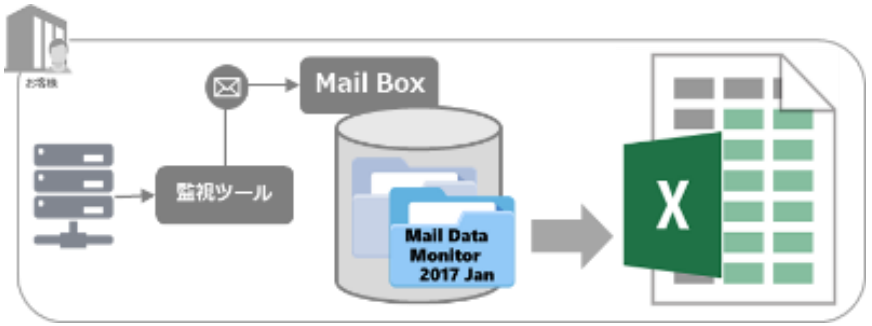
1．導入効果予測の可視化

2．社内稟議　説明資料

SHERPA-IR導入アセスメントの流れ

1. アセスメントお申込み

2. お客様のアラートメール
   データ送付



3. 想定効果レポートを提示

END

ご清聴ありがとうございました