北海道自治体向けクラウドサービスでのZabbix導入事例とOSS連携のご紹介

平成29年11月17日

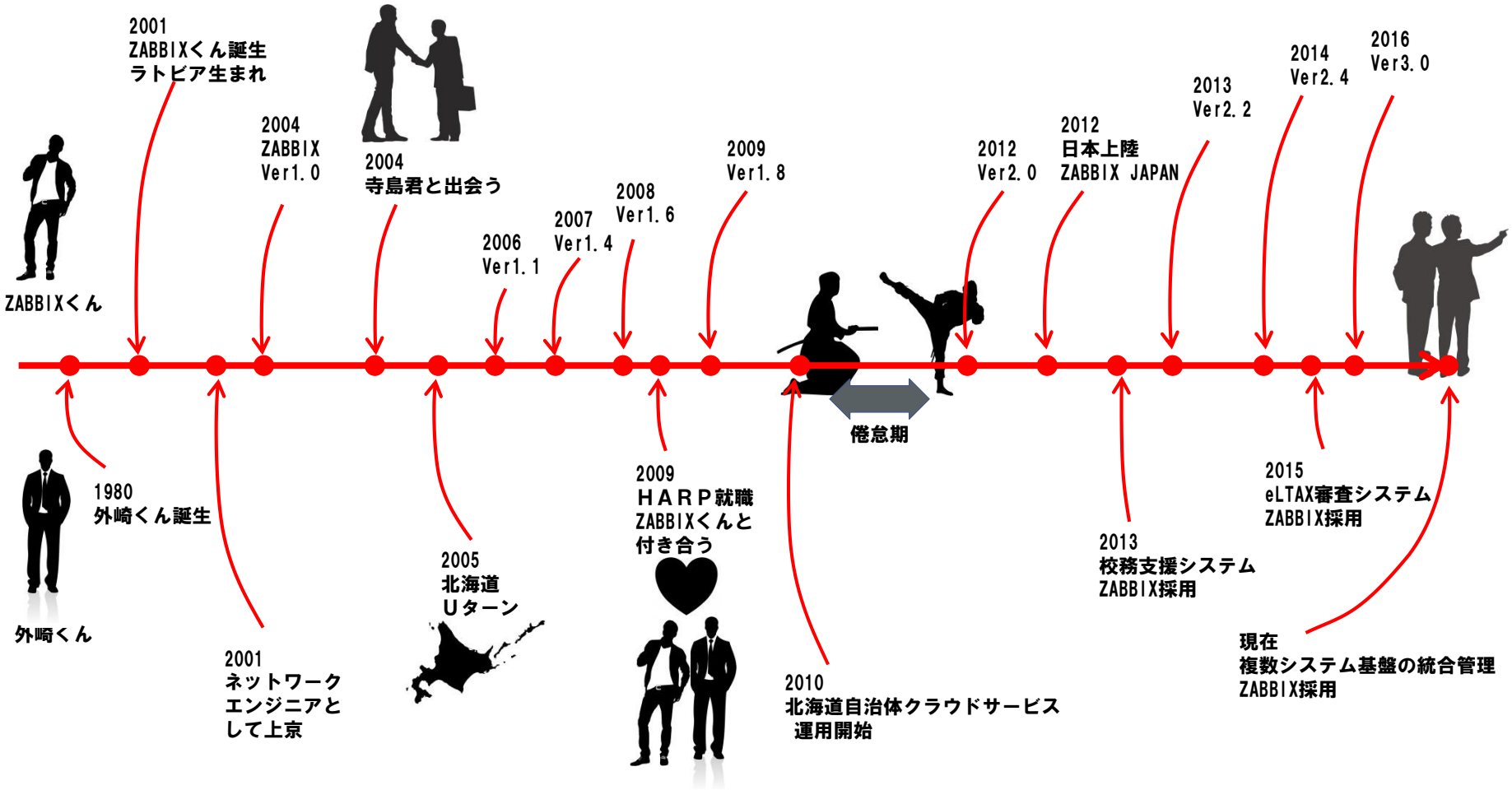
株式会社 HARP

自己紹介

- 外崎　幸大
- 北海道　富良野出身
- ネットワークエンジニア
- 子どもは３人います
- 最近の趣味はInstagramと革細工

自己紹介

ＺＡＢＢＩＸと私の思い出年表



会社概要

項　　目	内　　容
商　　号	株式会社ＨＡＲＰ
本店所在地	札幌市中央区北１条西６丁目１－２　アーバンネット札幌ビル３階
設　　立	平成１６年９月２１日
資　本　金	資本金　４７１，０００千円
主な出資者	・北海道　・ＮＴＴ東日本　・北海道電力グループ　・北洋銀行グループ　・北海道ガス
事業内容	・情報システムの企画、設計及び管理運営 ・情報収集・処理の提供サービス ・コンピュータシステム構築のコンサルティング業務 ・コンピュータソフトウエア・ハードウエアの開発、販売 ・システムインテグレーション（総合的なコンピュータシステムの構築及び保守）業務 ・コンピュータシステム構築の教育又はプログラムの設計技術者の派遣 ・前各号に付帯する一切の業務
セキュリティ認証等	・平成１８年２月１０日、ＩＳＭＳ認証基準（Ver.2.0）認証取得 ・平成１８年２月２１日、プライバシーマーク認定取得

Zabbix導入前（運用環境の課題）

導入前の課題

- サービス毎に監視ツールが導入され管理が煩雑
- 有人監視オペレータの監視レベルにばらつきがある
- 一元的な監視ができず、障害の特定に時間がかかる

The Webalizer
What is your web server doing today?

MRTG
MULTI ROUTER TRAFFIC GRAPHER

Tivoli

監視システム導入の選定方針

- 監視ツールを統一
- 監視水準の統一
- 監視運用の効率化

ZABBIX

なぜZabbixを採用したのか

・ＯＳＳ積極活用しコスト減の取り組み

・トライ＆エラーが許される状況だった

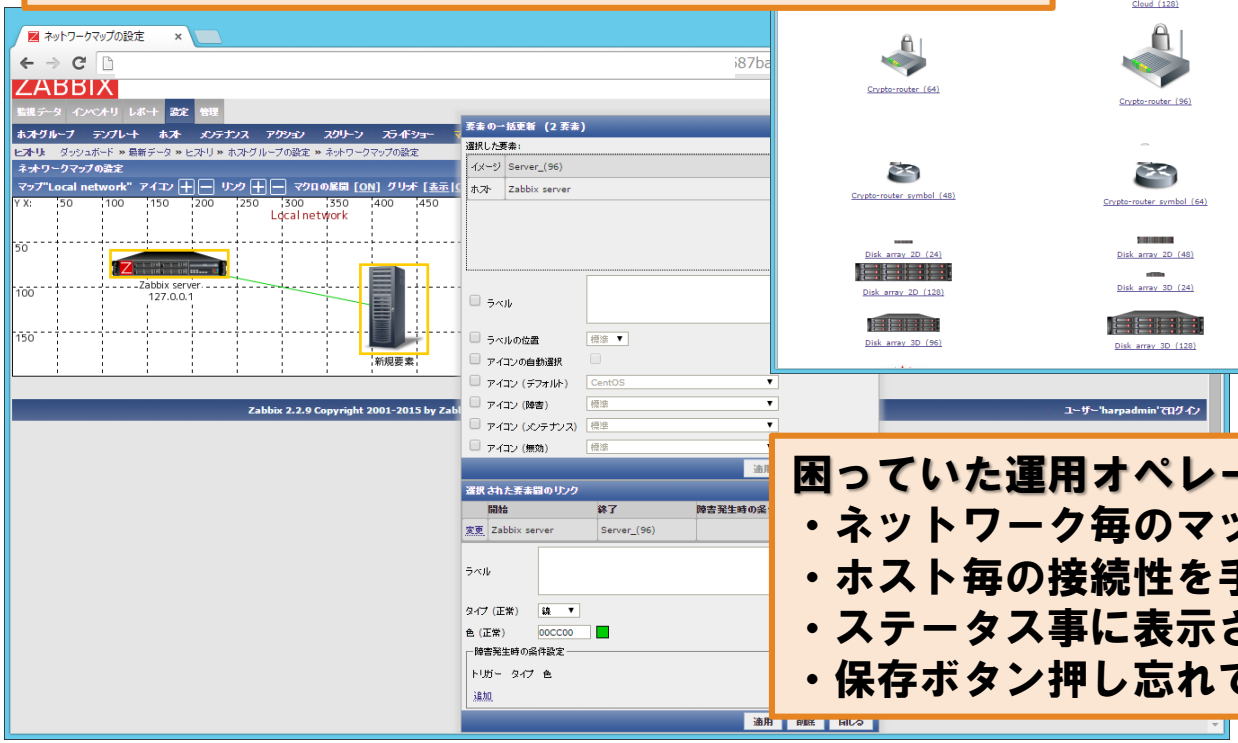
・特定のベンダーに依らない自治体主導の電子自治体の提供

・コミュニティの活発さと、寺島君の友情サポート

Zabbix導入後の課題①

課題・・・監視マップの作りこみが大変

困っていた運用オペレーション
- ホスト種別分のアイコンを作る・探して見繕う
- 正常・異常要アイコンを登録する
- マップのインポートもエクスポートもできない



困っていた運用オペレーション
- ネットワーク毎のマップにホストの台数分を登録
- ホスト毎の接続性を手動で設定
- ステータス事に表示させたいアイコン設定
- 保存ボタン押し忘れて１から作成しなおし・・・

Zabbix導入後の課題②

課題・・・監視ホストの登録が手動登録大変

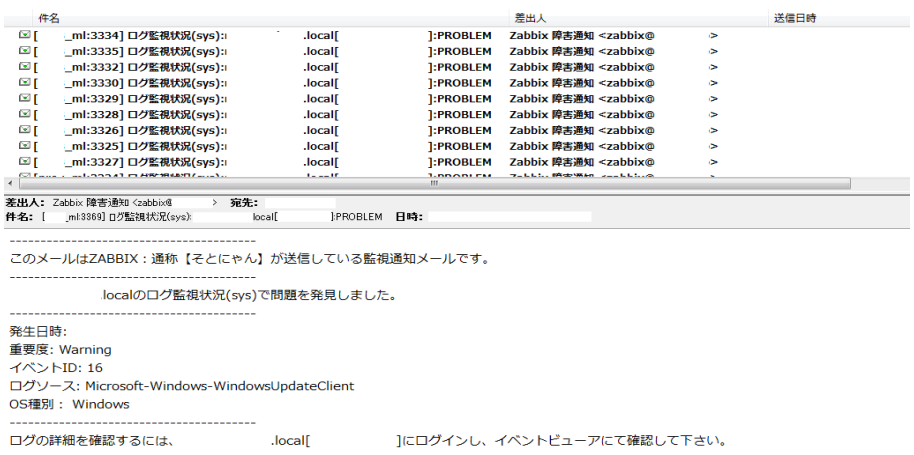
困っていた運用オペレーション
- 表示名やホスト名、アドレス情報等を手入力
- 対象ホストの数分繰り返し登録作業が必要
- 監視テンプレートはあるが、適用作業もそれなりに大変

Zabbix導入後の課題③

課題・・・監視登録直後にWindowsのイベントログアラートが大量に通知

困っていた運用オペレーション

- ＷＩＮＤＯＷＳイベントログ監視で「ＷＡＲＮＩＮＧ」は全部トリガ
- トリガされたイベントで警告異常はメール通知
- 金曜日監視テンプレをＷＩＮＤＯＷＳグループ全体に適用して帰社
- 月曜日出社すると、アラートメールが数千通・・・



課題の原因

初回の監視はログ行頭からチェック→１行目から最終行までをチェック
結果、過去数か月分のログ内容から、全ＷＡＲＮＩＮＧを通知することに

Zabbix導入後の課題④

課題・・・トラップやログ監視で短期間に複数の障害を検知すると誤検知

監視取得値

jul 18 13:00:29 host01 kernel: xxx: **error**=1234
jul 18 13:00:29 host01 kernel: xxx: **error**=5678

検知条件

log[/var/log/messages,error|Error]

アクション メール通知

{EVENT.TIME}に{HOST.NAME1}の{ITEM.NAME1}で障害が発生しています。
監視取得値：{ITEM.VALUE1}

困っていた監視結果
2通のメール通知、監視取得値の内容が違う

1通目	13:00:29にhost01のメッセージログ監視で障害が発生しています。 監視取得値：kernel: xxx: **error=5678**
2通目	13:00:29にhost01のメッセージログ監視で障害が発生しています。 監視取得値：kernel: xxx: **error=5678**

課題の原因
メッセージの取得精度の問題で、ログデータをメールのメッセージ内に取りこめない場合があった

Zabbix導入後の課題⑤

課題・・・クライアント証明書対応のＷＥＢページ監視ができない

認証タブがない

フォーラムで聞く
Web監視の機能でなんとかできないか・・・
Curlが裏で動いてるらしいことを知る

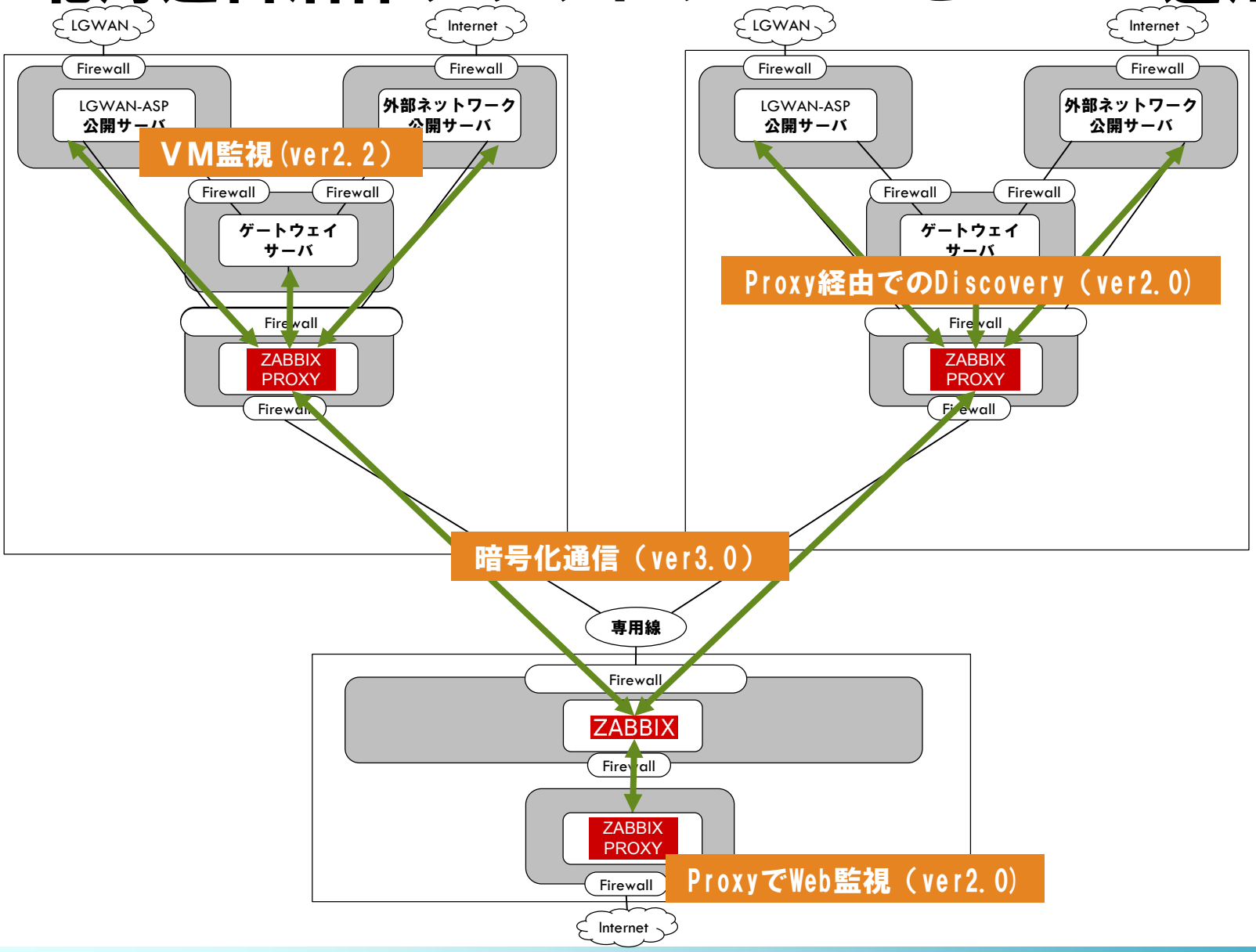
困っていた運用オペレーション
ユーザーパラメータを使用して乗り切る

```
web.check[*],curl -L -i --connect-timeout 15 --cert xxxcrt.pem --key xxxkey.pem $1 |egrep "$2" |wc -l
```

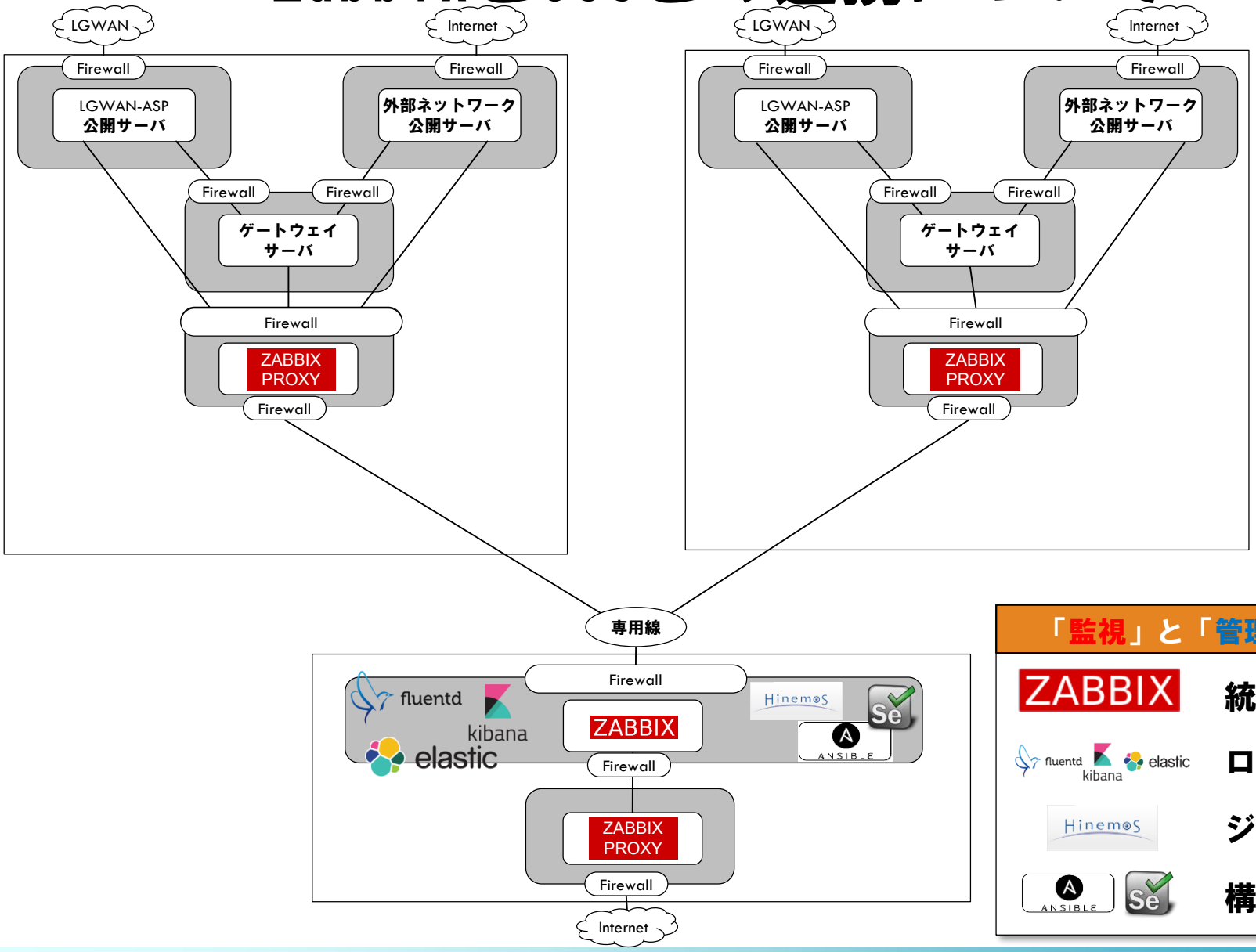
Zabbix導入後の課題は勝手に解決！

監視マップの作りこみ	ZABBIX Ver2.0	アイコン自動マッピング ホストグループ内ホスト登録
監視ホストが手動登録	ZABBIX Ver2.2	アクティブＡｇｅｎｔ自動登録
ログ監視アラートが大量通知	ZABBIX Ver2.0	Eventlogアイテムにmodeパラメータ登場
短期間での複数障害で誤検知	ZABBIX Ver2.0	監視値の取得精度がナノ秒対応
ＵＲＬ監視がクライアント証明書非対応	ZABBIX Ver2.4	クライアント証明書対応

北海道自治体クラウドサービスとZabbix運用環境



ZabbixとOSSとの連携について



「監視」と「管理」を区別

ZABBIX 統合監視

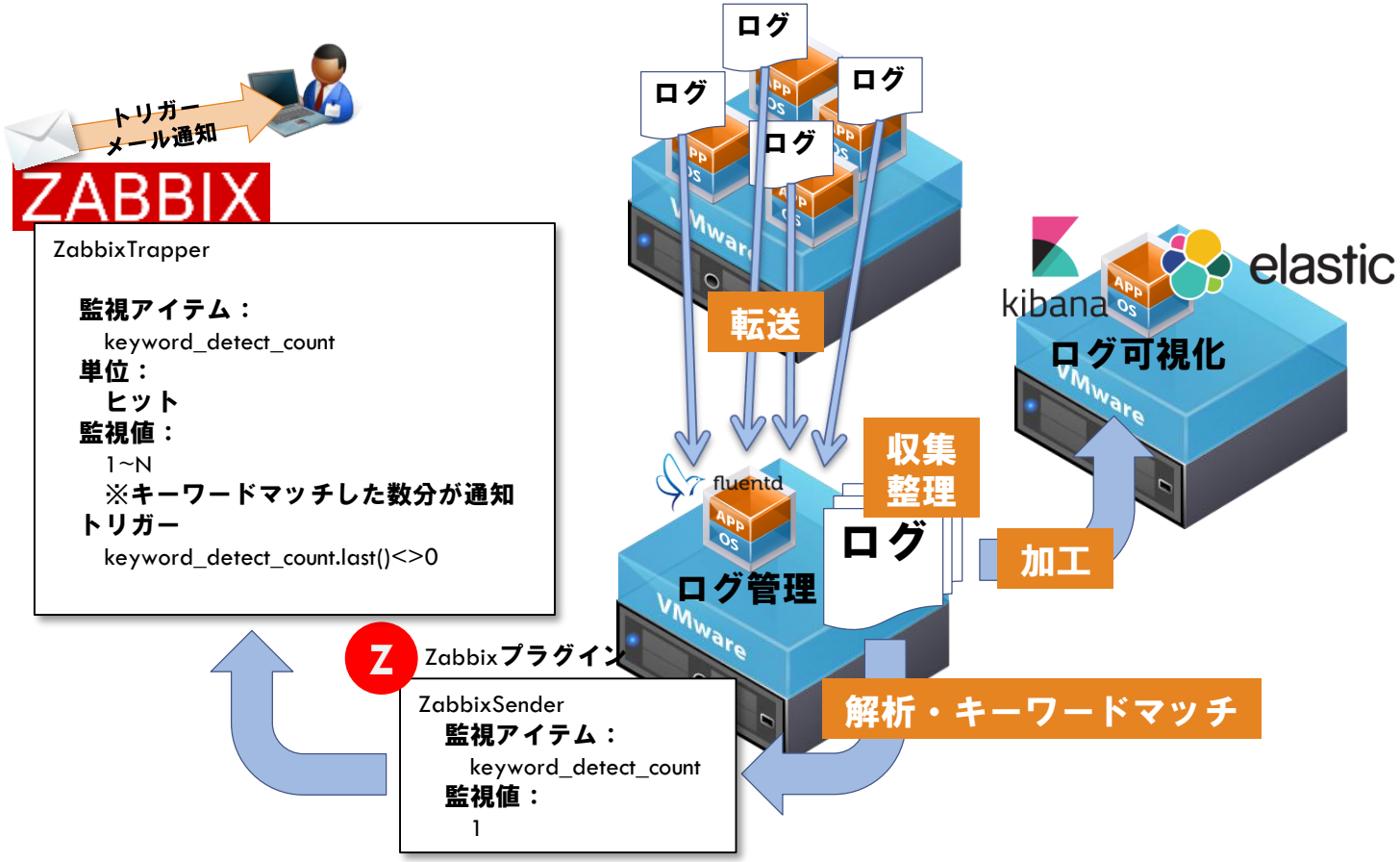
fluentd kibana elastic ログ管理

Hinemos ジョブ管理

ANSIBLE Se 構成管理

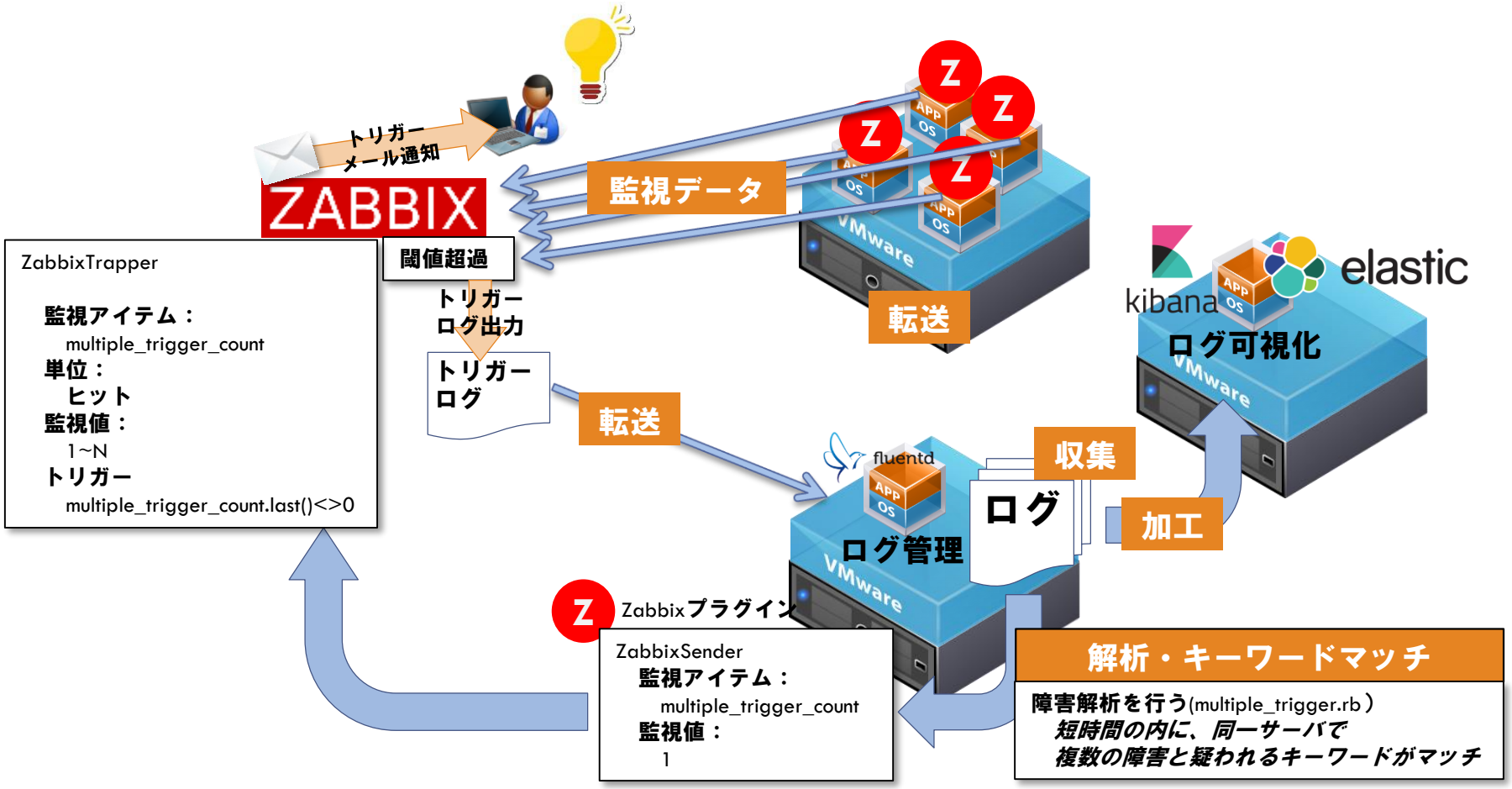
Zabbix＋fluentd+kibana+elasticsearch

ログ収集はFluentdで実施し,情報の整理はKibanaとelasticsearchが担当
収集ログの解析はFluentdで行い、解析結果をZabbixに送信



Zabbix＋fluentd+kibana+elasticsearch

ログ解析が得意なFluentdと連携する事で、高度な監視を実現



Zabbixの良いところ（私見）

他システムの連携性

OSSの性質上、仕様が公開されていることもあり、他システムとの連携に関する情報が広く普及している

サポートが充実

質の高いコミュニティが活発（日本Zabbixユーザ会）

実装レベルで解決可能な有用な情報が満載

リリース計画

ニーズに遅れる事なくリリース対応

計画されたリリース対応が将来に安心感

ノウハウの蓄積

統合監視ツールは多機能な反面、ノウハウの習得が大変

監視テンプレートという形でノウハウが残せる

アップグレードでも操作方法は変わらない

今後に期待すること

テンプレートやディスカバリ等一括で追加された監視アイテムに対する変更が苦手

ZABBIX Ver？

WindowsOSコマンド実行結果をエンコード

ZABBIX Ver？

Web監視のSSLピア検証でメモリリーク

ZABBIX Ver？

ZabbixProxyの成長

ZABBIX Ver？

いつ頃かな？