show techはコワクナイ

(続show techってナニモノ？)

JANOG40
株式会社シーイーシー 三ツ木絹子
mitsugi@mex.ad.jp

JANOG22

- プログラム応募の意図
  - 障害解析時、show tech-support を要求されることへの不満と不安
  - show tech-support をとることの意義ってナニ？
  - メーカさん、ユーザの気持ち、わかってる？
  - お互い歩み寄れるところないのかな？
  - もっと気分良く show tech-support とって、早く解決に結び付けたい！！

show tech はムダではないことがわかった

- 当日の議論から
  - ユーザのレベルがどうであれ均一な情報を取得できる
  - ログ以外の重要な情報を取得できる（メモリ番地とか）
  - 他のプロセスになるべく影響を与えないよう優先度は落としている
  - コマンドの発行順位を重要な情報を取れる順にすることで、万が一途中で落ちたとしても解析しやすいようにしている
  - （でも、もうちょっとメーカも考えた方がいいかもって思ったとのコメントも）

programも
ムダではなかったことがわかった!

- プログラムの後、体感したこと
  - show tech-support を提供せずに対応してもらえるケースが出てきた
  - show tech-support をとることで機器に与える負荷を質問すると、その危険度について答えてくれるベンダが出てきた
    - 以前は「show tech-supportが無いと保守できない」の一辺倒だった
  - 落ちるかもしれないが show tech-support を打たないといけない場合でも、メーカさんも考えてるし「これで落ちたら仕方ない」と多少思えるようになった!

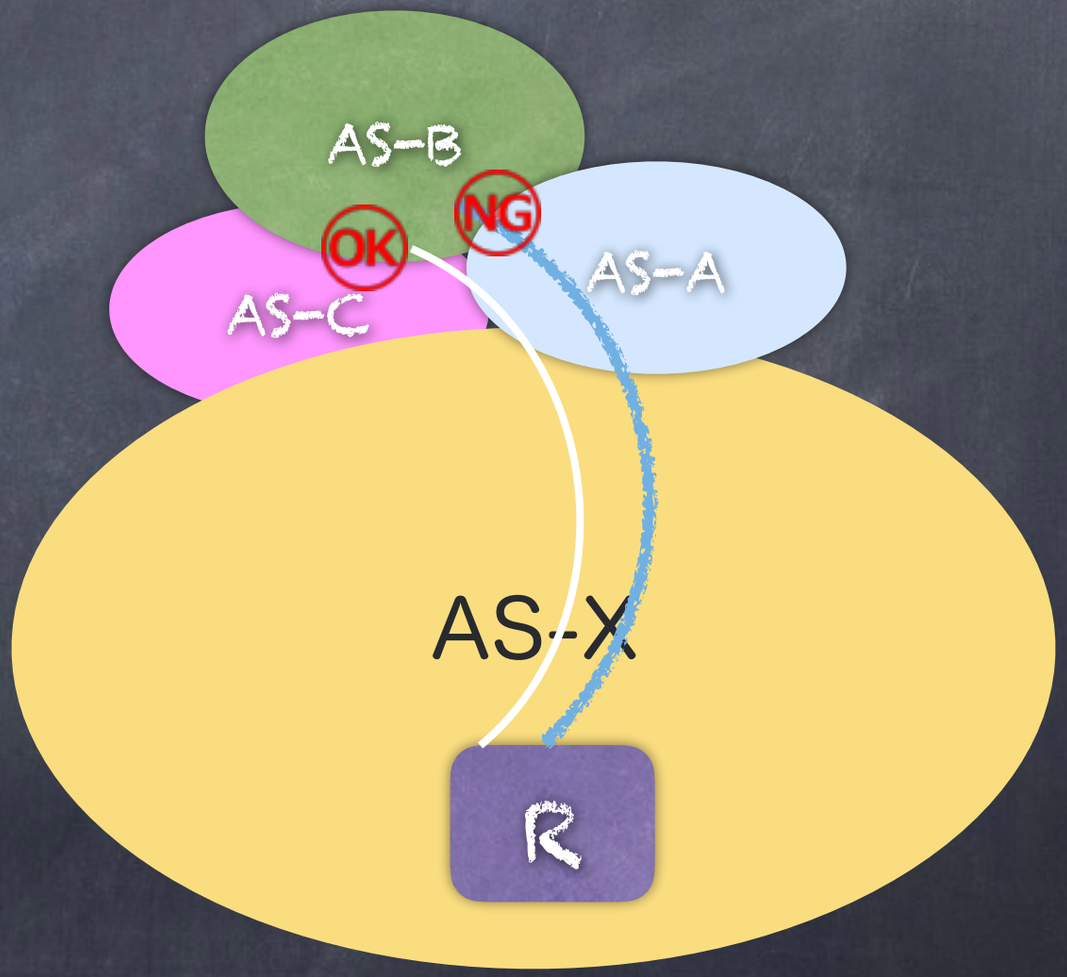
JANOG40

早いもので、あれから10年近くが経とうとしています

- あれからメーカさんはどんな工夫をしているのだろうか？
- 障害解析のためのユーザの手間（ひいては復旧までの時間は）軽減されたのだろうか？
- show tech-support を要求されることへの不満と不安は解消されたのか？
- 更に追加で問題になってきたことはないか？

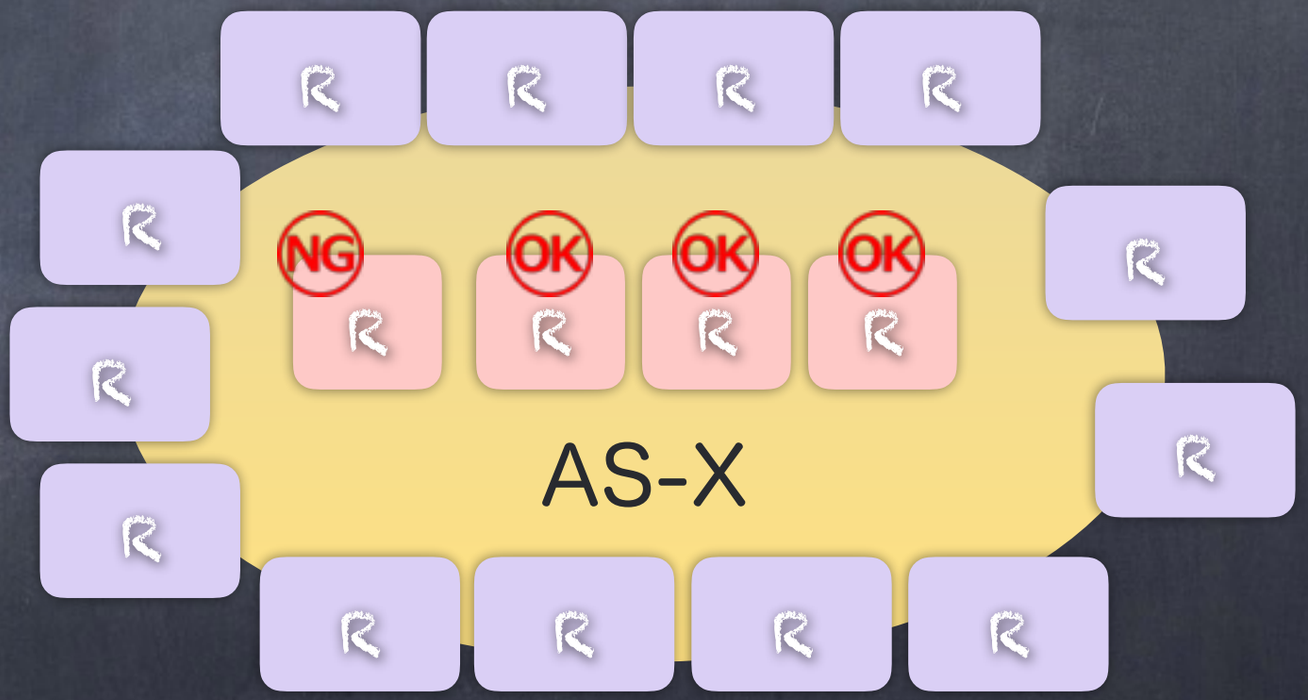
障害対応とあるケース

- 自網内のルーティング障害
  - 特定の自社 prefix と特定の外部 prefix 通信のみ通らないように見える
  - ボーダルータで見ると経路はある
  - src address, dst address から traceroute をとったり



障害は復旧したものの

- あるルータが原因であることを特定でき復旧
- 次は障害の「本当の」原因調査
- NG ルータの show tech-support を採取して保守ベンダに送付、解析依頼を行った



show tech で解決したか？

- NG だったルータの show tech-support だけでは解決しなかった
  - 初めて見るコマンド多数でも論理的に切り離した環境なので心穏やかに対応できたらしい
- 経路情報に問題があるため、隣接ルータのすべての show tech-supportが必要になった
  - 2,3台ならともかく、何台あるんだー…
  - 今の情報でわかるのか？
  - 隣接ルータの機種は色々だけど、解析できるんだろうか？
  - 他ASとのpeerで同じ事象が起きたら情報もらえないよなぁ。。。

隣接ルータのshow tech で解決したか？

- NG だったルータの保守ベンダだけでは解決しなかった
  - 他社機器の機能や利用パラメータについて、情報が公開されていない等
- 結局、隣接ルータの保守ベンダにも問い合わせ
  - なぜ、そんな問い合わせをしているか、という経緯を説明したり
  - 今まで取得したログ類を送付したり…

  ということの繰り返し。

でも、解決のために他社製品の情報確認までしてくれるのは感謝だと思う

この時思ったこと

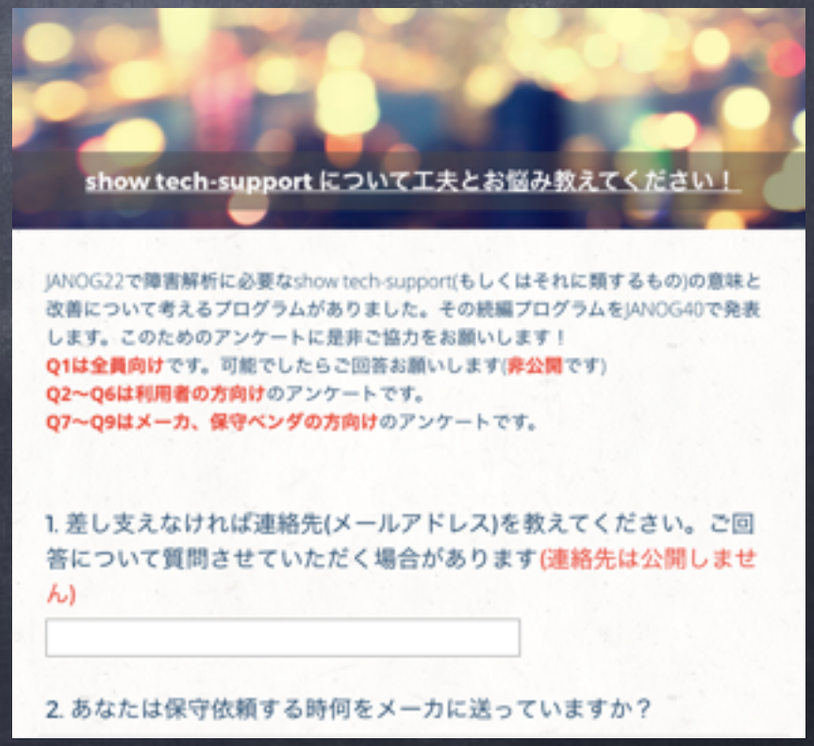
- マルチベンダ化に関して
  - show tech-support があって良かったんだと思う
  - 他ベンダの保守チームが一通り状況を確認するのに足りる情報が網羅されていた
    - ただし、バグやルーティング障害の解析時は、show tech-support は「取っ掛かり」
- 周辺情報の必要性
  - 必要なのはわかるが、手間も提出するデータ量も格段に増える
    - upload　サイトが無い所からは分割して送ってくれと言われるとさらに手間
  - 復旧の目処がたっていない場合はエンジニアにはかなりの負荷
- 復旧優先したい。物理的に切り離したら問題の情報は取れず、障害の解析はできなかった

他のみんなはどうしてい

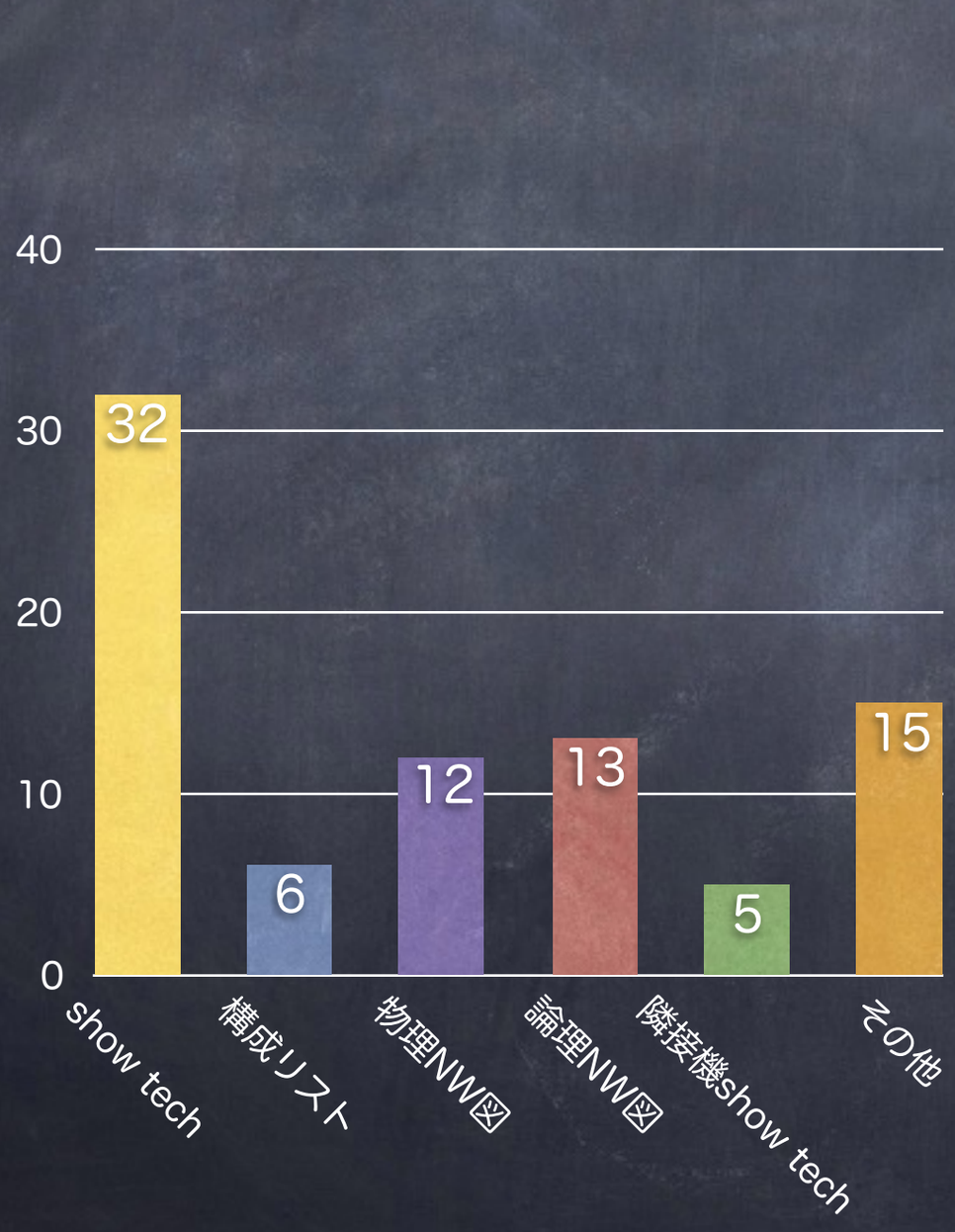
るのだろう？

アンケートを行いました

- show tech-support を取得する際に注意していること、工夫、困っていることなどを質問
- 期間: 2017/07/12~23
- 43名の方にご回答いただきました
- ご協力くださった皆さんありがとうございます！
- アンケート結果のご紹介はこの後
- すみません。多少意訳しています！

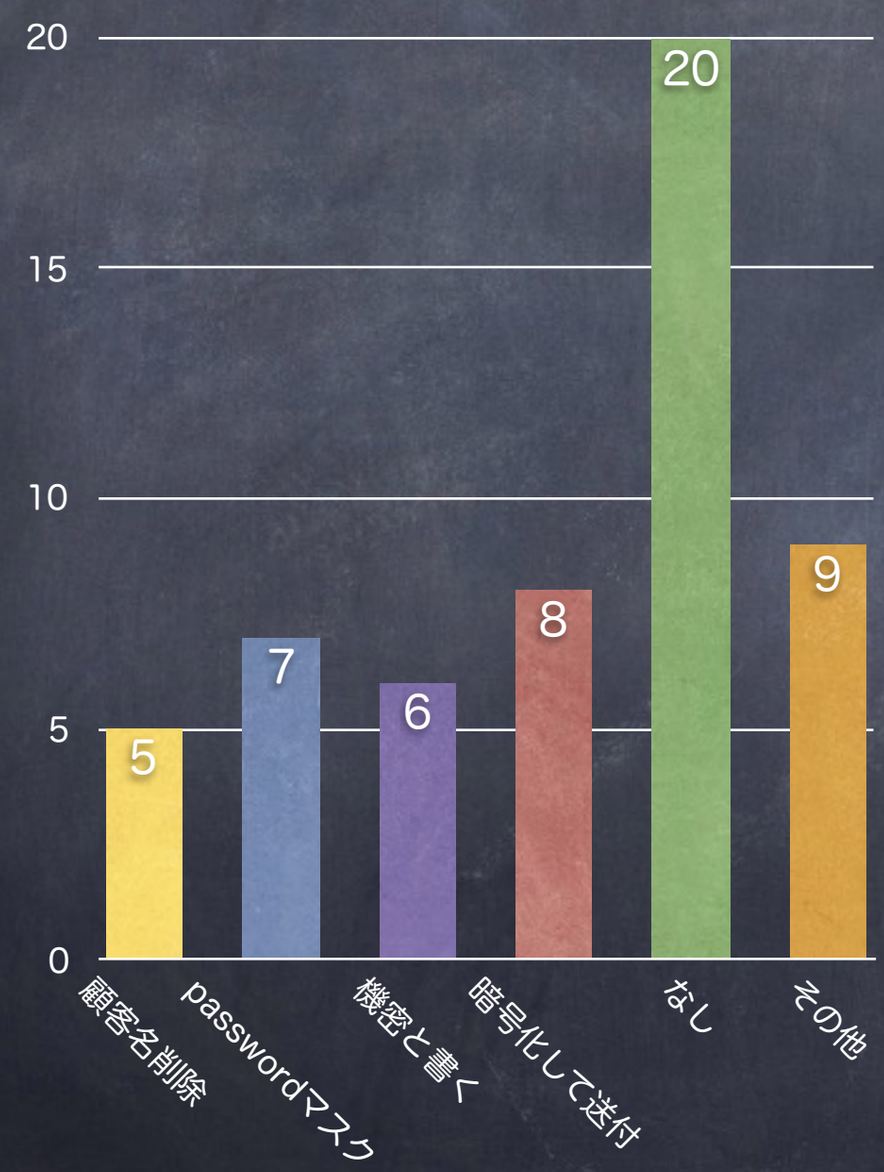


Q2: あなたは保守依頼する時何をメーカに送っていますか？



- その他
  - ライセンス情報
  - まずはログ
  - 経路情報やNATのセッション情報など「生の情報」
  - リソースの利用情報
  - リソースやトラヒックなどの推移のわかるグラフ
  - メーカが希望したもの
  - 作業手順など
  - コンフィグ
  - コンフィグや構成図を事前共有している方も

Q3: show tech-support を送る時に気をつけていることはありますか？



- その他
  - 極力そのまま送る
  - メール添付ではなく、クラウドストレージ的なもの経由で送る
  - メールで送信する時は圧縮かつパスワードをつける
  - IPアドレスをマスクする
  - 保守契約締結時にNDAが結ばれているのでそのまま
  - 内容を確認できないものは送れないので show techは送れないことがある

Q4: show tech-support を取得時に困ること、困ったことはありますか？

- 送付方法。大容量でも対応可能な暗号化して提供可能なファイル転送の仕組みがあると嬉しい
- CPUやメモリの消費をするコマンドがあり、気をつけている。もしくは不安になりながら実行している。あるいはお客様に影響が出た
- show tech でrebootしたことがあり、show techが鬼門になっている
- show tech の中にバグを踏むコマンドが入っていた
- シリアルコンソールから実行したところ完了に時間がかかり、それまで他のコマンドを受け付けなくなった
- SSH経由でとってCPU負荷が上がってしまった
- full route が出力されてしまい、えらい目にあった (*_*)
- show tech のデフォルトの出力先が HDD だったり画面だったりでびっくり
- HDD 上にできたファイルを手元に移動、それをメール、と手間。CPU 負荷も上がっていそう
- 役に立つ情報が取れているのか？と思う

Q5: show tech-support を取得する際(もしくは事前に)工夫していることは？

- 実環境で実行前に負荷をメーカに確認。あるいは、検証環境で実施する
- 冗長系の場合は、正副同時に実行はしない
- 負荷の少ない時間帯に実施する
- CPU利用率、通信量など総合的に影響を考えて実行タイミングを決める
- show tech-support を分解して個別の show コマンドで実行する
- terminal length 0 とか | no-more などで改ページしないようにする
- CLI だと時間がかかるので、フラッシュメモリへリダイレクト
- 大量のログに備えてターミナルソフトでログをファイル出力させる
- show tech-support 以外のコマンドを追加で要求することが多いので必要そうなコマンドをカスタムスクリプトとして先に作っておく
- 取得後のログのCRを消してLFだけにする
- ログ取得用のウィンドウは作業ウィンドウとは別にする
- 覚悟して打つ
- 重いだけで提出できないので show tech-support は取らない

Q6: 運用上(過去の失敗から)、実行禁止！となっているコマンドや操作があったら教えてください

- 障害になった・顧客影響が出た系
  - debug
  - debug の乱用
  - show tech-support
    - セッション情報を頻繁に更新しそうなコマンド
    - 古い OS で full route を出力するようなコマンド
- 念のため系
  - 実績のないコマンド
- その他
  - C社さんルータで、コンフィグモードからCtl+z で抜けたり、リターン連打（y/n を聞かれているのにデフォルトで通ってしまう)
  - show cdp neighbors detail

Q7: 負荷低減のためのOSやCPUアーキテクチャに関する工夫を教えてください

- 古河ネットワークソリューションさん
  - トラヒックの中継を妨げる可能性のあるログ取得はしない
  - トラヒックの中継を妨げるくらいならログ情報の方を落とすように負荷のかからない仕組みを取っている
- IIJさん
  - CPUが高負荷になっても機器の動作に影響しないような仕組みを採用
- ARISTAさん
  - プロセス間通信を軽くし、また、プロセスは状態を持たないようにしている
  - 全体を管理するSysDBが状態を保持しており、CLIもSysDBにアクセスするのでプロセスへの影響がない

Q8:ログ取得コマンドで改善をしている点があれば教えてください

- 古河ネットワークソリューションさん
  - 出力情報が多くなったので、画面出力だと遅いため、ファイル出力できるようにした。ファイル出力したものはftpで提出
- IIJさん
  - 出力項目が多くなった。ルータ管理システムで統合管理可能。USB ドライブに保存も可能
- CISCO さん
  - show tech の後ろにサブコマンドをつけることで部分的な情報取得ができるようになった
- ARISTAさん
  - 定期的(1時間毎)に取得してHDD内に保存、圧縮。様々なredirectionが使えるのでgithubなどに食わせるとかも可能
- Brocadeさん
  - supportsave でコンソールへの出力なしに、より多くの情報を得ることが可能

Q9:show tech-supportの裏技、オススメの方法があったら教えてください！

- show tech-support は、どのような環境で何が起きたかを知るための第一歩。保守会社と、ケースバイケースで利用するコマンドとその影響度について事前に話し合っておくと良いのでは
- Juniper さん
  - SSH でアクセスしてログを取るのだと暗号化で CPU に負荷をかけるのでログをリダイレクトでファイル出力する（コンソール出力させない）のがオススメ
    - ハードウェア障害をトリガーとして事象発生時のログ出力させるようにスクリプトを書くことが可能(EventScript)
    - スクリプトを使って機器に個別にログインすることなくログ取得することが可能
- Arista さん
  - CLI とスクリプトでログやコマンド実行をスケジュール　(CLI Scheduler)
  - イベントトリガーでスクリプト実行 (Event Manager)
  - 重要なシステムイベントをローカルのSQLite データベースに保存 (Event Monitor)
- NDA を結んでいるのだから、パスワードや顧客名は気にせず送って良いのでは？早く解析しよう！

会場から

ご意見ください

- 情報収集コマンド
  - こんなところが助かっている
  - 嫌い。困る
  - 工夫の紹介、こう使うといいよ
  - 保守ベンダとのやりとりのノウハウ
- メーカの方
  - コマンド、アーキテクチャ面で工夫の紹介を
  - 取得した情報の編集などで困ったことはありますか？
- その他
  - 斬新なアイデアなど、なんでも！

会場からのご意見
（ありがとうございました！）

- 情報収集コマンドで利用されることの多いマネージメントモジュール上のバスでロックアップしないような仕組みをJuniperは取り入れている
- ログを採って障害解析したいけれど、復旧がやっぱり優先。メーカがハード障害をトリガにログを吐くスクリプトを提供してくれたら嬉しい
- show tech-support は障害解析のきっかけ。どのような機器とつながっているかといった環境の情報や、障害が発生するトリガとなる事象はなかったか、など、保守ベンダに伝えてコミュニケーションをとることで障害解析が迅速になる
- 定期的に show tech-support が取られていれば、障害後に show tech-support をとることでリブートしてしまうという心配をしなくて良いので、いろいろなメーカで実装してもらえたら嬉しい
- ログのリダイレクト先が豊富になってきたので、採取したログを直接アップロードできるようなサイトを準備してもらえたら便利
- show tech-support をすることで、ユーザと保守ベンダのやりとりを少なくすることはできるが、サポート体制によっては、もっと軽いコマンドや周辺情報を聞く方が早く障害解析できることも多い
- マルチベンダでの障害解析のボトルネックにならないようにした上で、NDAやコンプライアンスを考慮した保守契約をする必要がありそう。情報があれば共有していきたい
- ユーザの現場が契約内容に含まれるNDA等を理解しておらず、ログ提出をしてもらえないことがある。保守ベンダも障害解析を速やかに行いたいので、現場の方は契約内容を確認しておいてくださいネ
- show tech-support をメーカサイトにアップロードすると、正常時とは異なると思われるメッセージの箇所がマークアップされるような仕組みがあったらイイナ！

まとめ

- 運用は経験・体験の積み重ねもあるので、過去痛い思いをした人は能天気にshow tech-support は打てないかもしれない
- show tech-support も、アーキテクチャも進歩してきている
- メーカはユーザの要望を取り入れる準備がありそうです！
- 「危ないコマンド」「治ったコマンド」などの情報共有は業界内でできるといいな
- でも一番は障害の起きない機器が一番いい❤️
- さて、次はJANOG60?! (なんちゃって)