Cisco IOSの2020年1月1日問題
その時何が起こったか？

JANOG45 Day2 LT
2020/1/23

佐々木 健

2020年1月1日問題の概要

- 2019年末に Cisco IOS/IOS-XE のバグが報告された
- 2020-01-01 00:00:00 UTC に自己署名証明書が期限切れになる
- この自己署名証明書を使用しているサービスは機能しなくなる可能性がある

ドキドキポイント

- アナウンスが直前
  - 初出は2019/12/17(2週間前)
- そういえば証明書期限切れによる大障害ってあったよねえ
- 2000年問題っぽさを感じる
  - 令和関係ないけど

ムムムポイント

- 本件の影響が良くわからない
- ネットワーク機器の証明書って真面目に管理しなきゃいけないものなのかな？
- 更新が必要なものって運用が面倒だよねえ

ニヤニヤポイント

- 現場はバタバタして大変だろうなあ
  - 運用者側も、開発者側も
- ひょっとすると予想外の大規模障害が発生したりするのかな？
- なにかあってもなくても、現場では内緒にしなきゃいけないのかな？
  - 立場上言えなかったり言いにくかったりとかありそう
  - しがらみとかもあるよね
- 私は今回はまったく関係がない、対岸の火事!!!

アハハハポイント

- CISCOの説明がとても爽やか

Q. この問題が発生した理由は何ですか。
残念ながら、テクノロジーベンダーの**最善の取り組みにもかかわらず、ソフトウェアの欠陥は依然として発生しています**。シスコのテクノロジーにバグが見つかると、シスコは、透明性を高め、お客様がネットワークを保護するために必要な情報を提供することに取り組んでいます。
この場合、問題は、Cisco IOS および Cisco IOS-XE の該当するバージョンでは、自己署名証明書の有効期限が常に 01/01/2020 00:00:00 UTC に設定される、既知のソフトウェアバグが原因で発生します。この日付を過ぎると、証明書の有効期限が切れ、無効になり、製品の機能に影響を与える可能性があります。
…
Q：2020年1月1日 00:00:00 UTC の有効期限が選択されたのはなぜですか。
通常、証明書には有効期限が設定されます。このソフトウェアバグの場合、2020年1月1日は、**10年以上前の** Cisco IOS および Cisco IOS-XE ソフトウェアの**開発時に使用され、人為的なミスです**。

2019年12月末

出して
ＬＴ

対岸から火の粉が
飛んできたよ、、、、

アンケートを取ってみました

- IOS/IOS-XEは何台くらい管理してますか？
- Cisco IOSの2020年1月1日問題を知っていましたか？
- 2020年1月1日になにかありましたか？
- 当日は待機等、特別な運用対応は行ないましたか？
- 事前に何らかの対応を行ないましたか？
- 今回の問題に限らず管理してるネットワーク機器およびサーバーが自己証明書を使ってるか把握していますか？
- 自己証明書の期限の管理をどのようにしてますか？
- 本件について何かあればコメントをお願いします。
- もし差し支えなければ、所属、お名前、連絡先を教えてください。個別に連絡をさせていただくかもしれません。

アンケート回答者総数

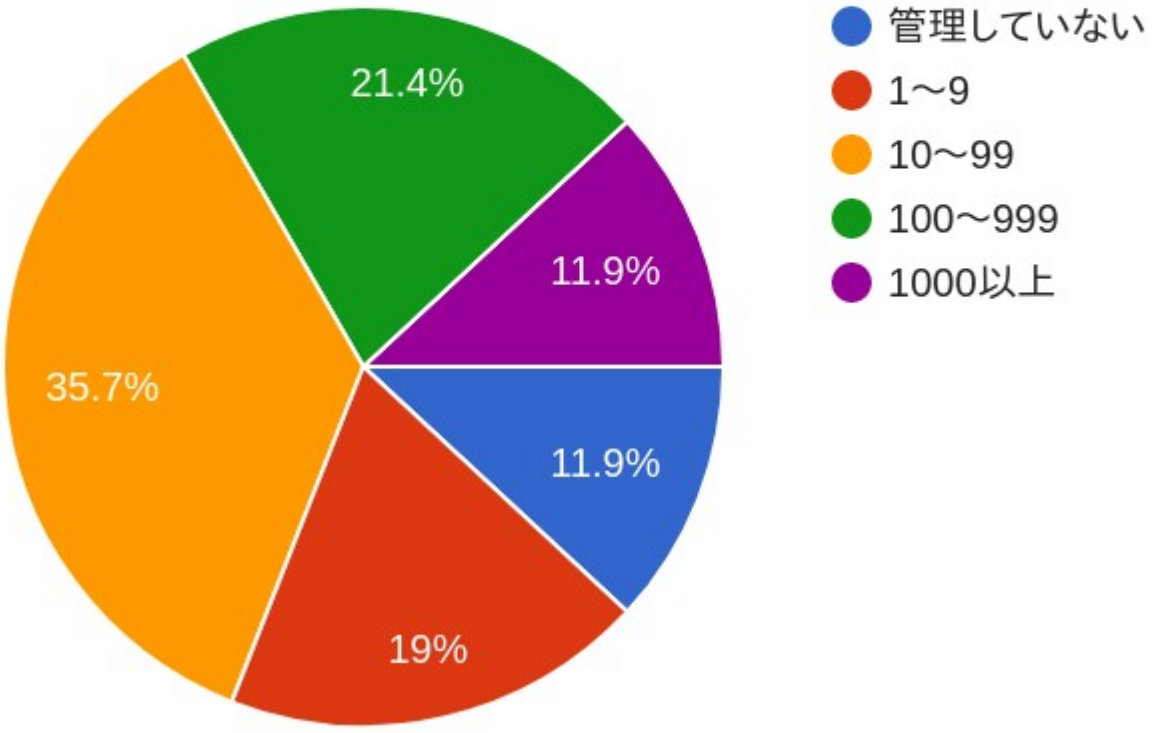
47名

ありがとうございました!!

回答者内訳(未回答者除く)

IOS/IOS-XEは何台くらい管理してますか？

42 件の回答



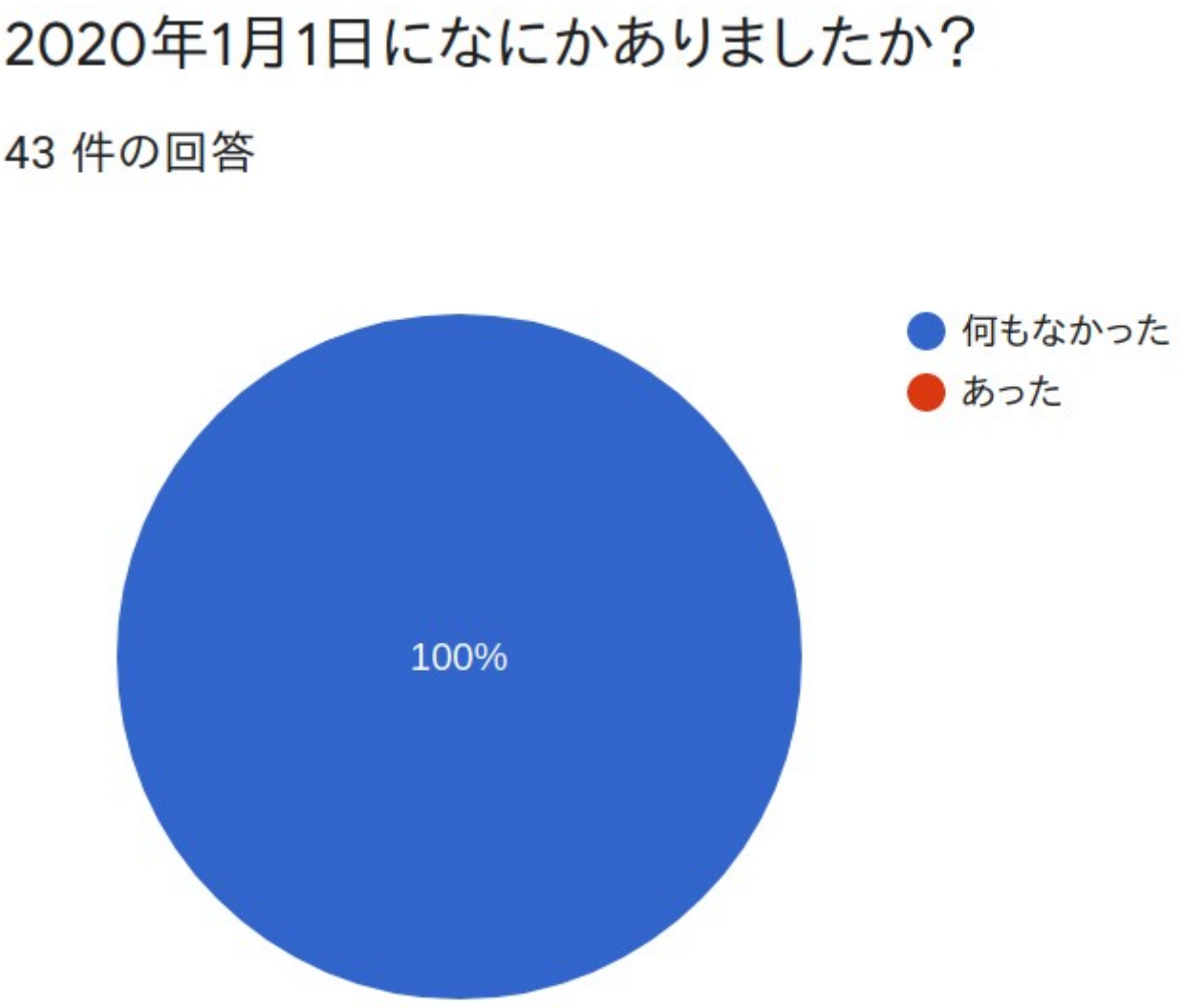
2020年1月1日に何かあったのか？

(どきどき)

2020年1月1日に何かあったのか？

(わくわく)

2020年1月1日に何かあったのか？



2020年1月1日に何かあったのか？

何もなかった!!!

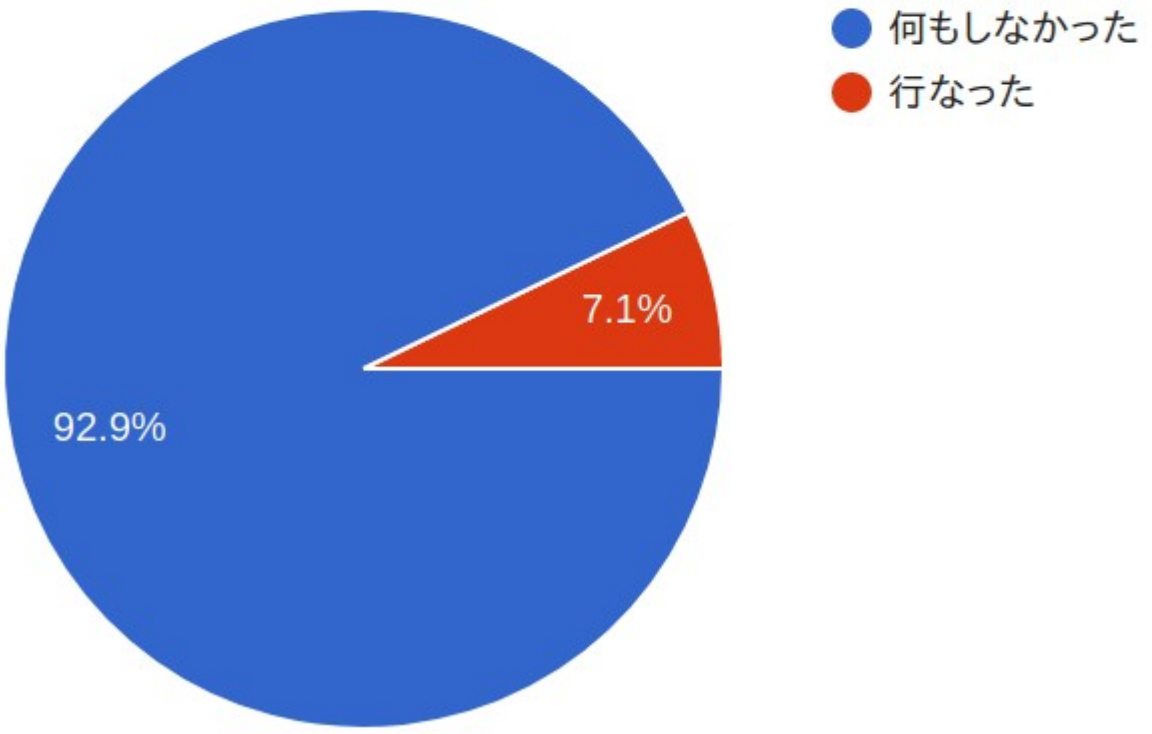
良かった!!!

(テンション下がりましたね)

(平和の陰で頑張った人もいる!!)

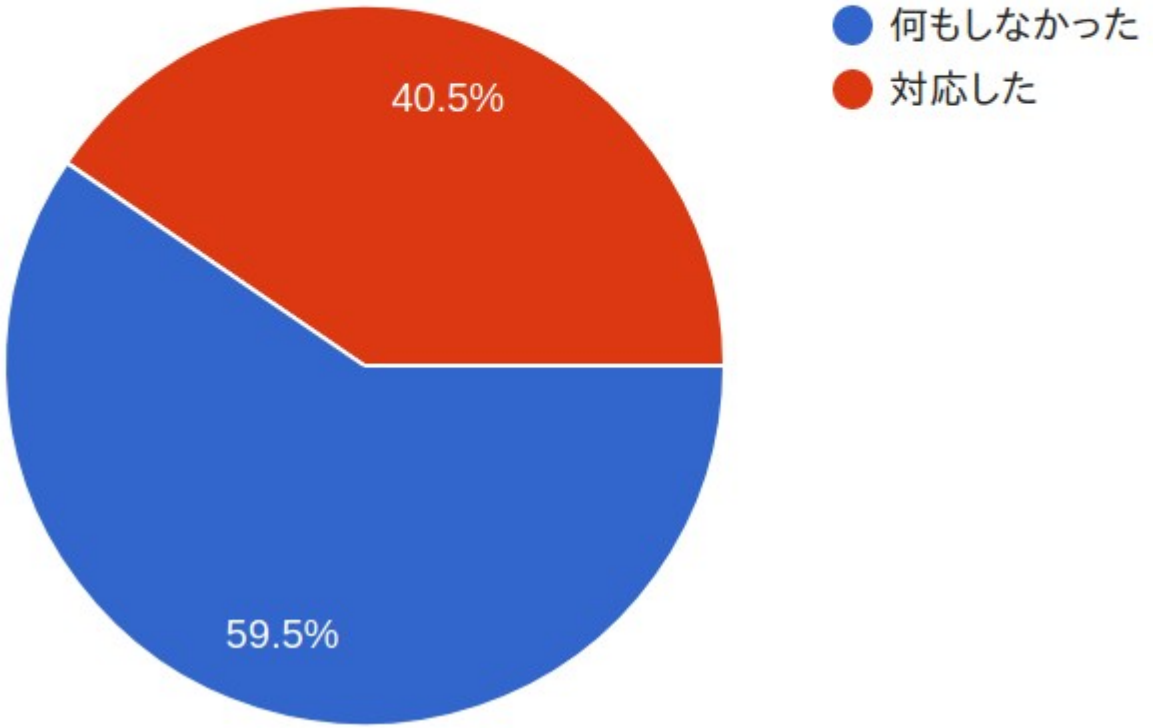
当日は待機等、特別な運用対応を行ないましたか？

42 件の回答



事前に何らかの対応を行ないましたか？

42 件の回答



当日/事前対応 その1

- 影響有無の確認(10回答)
- 自己署名証明書の利用調査(2回答)
- 関係者に連絡、事前周知(2回答)
- エスカレーション体制構築
- 保守窓口の増強
- 監視強化
- 1月1日リモート待機

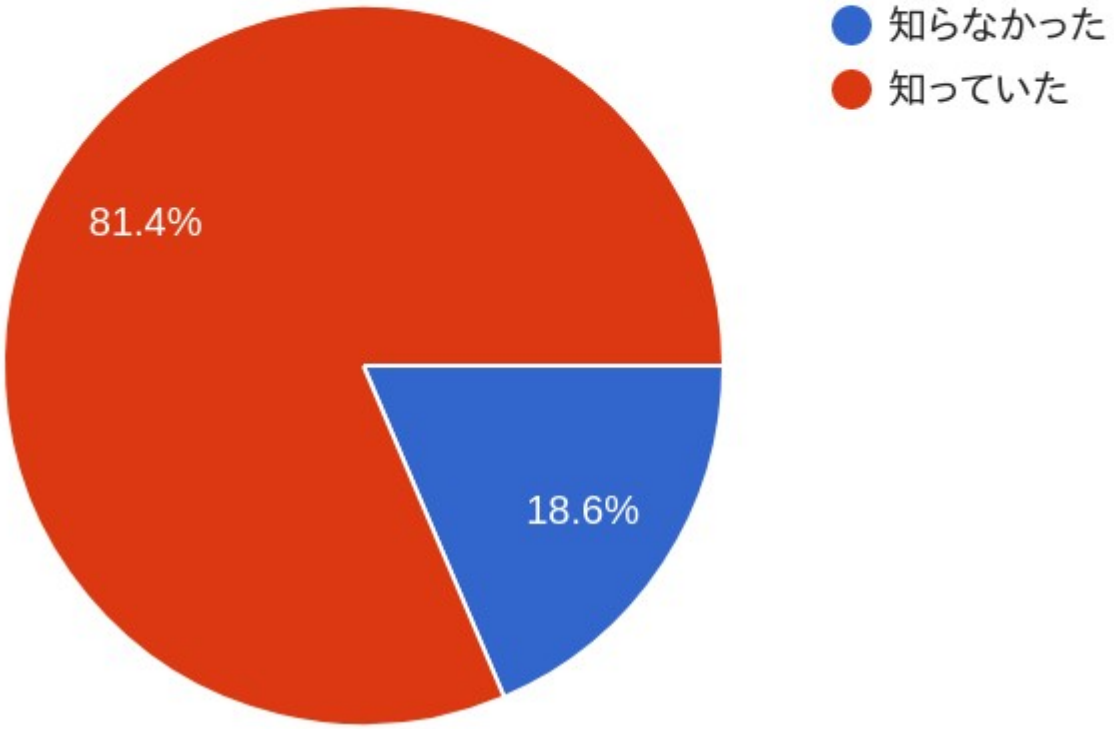
当日/事前対応 その2

- 影響あるかどうか良く分からなかったので、実際に影響があった場合の業務影響を洗い出し、何か発生した場合にも代替の通信手段があり、(幸いにも)正月休み明けの事後対処でも業務にクリティカルな影響がないことを確認した。で、結局、何もしなかった。
- WLCとAP間の接続で利用している証明書があり、回避設定を追加。実際には製造から10年の期限で、1/1とは関係が無かった。
- 管理してるコンフィグから対象の洗いだし、アップデート
- OSアップデート実施 実施できない奴は放置
- no crypto pki trustpoint TP-self-signed-XXXXXXXXXXの実行
- no ip http secure-serverの徹底：デフォルトのまま上がり続けていた機材が数%あった（苦笑

（この問題って知ってた？）

Cisco IOSの2020年1月1日問題を知っていましたか？

43 件の回答



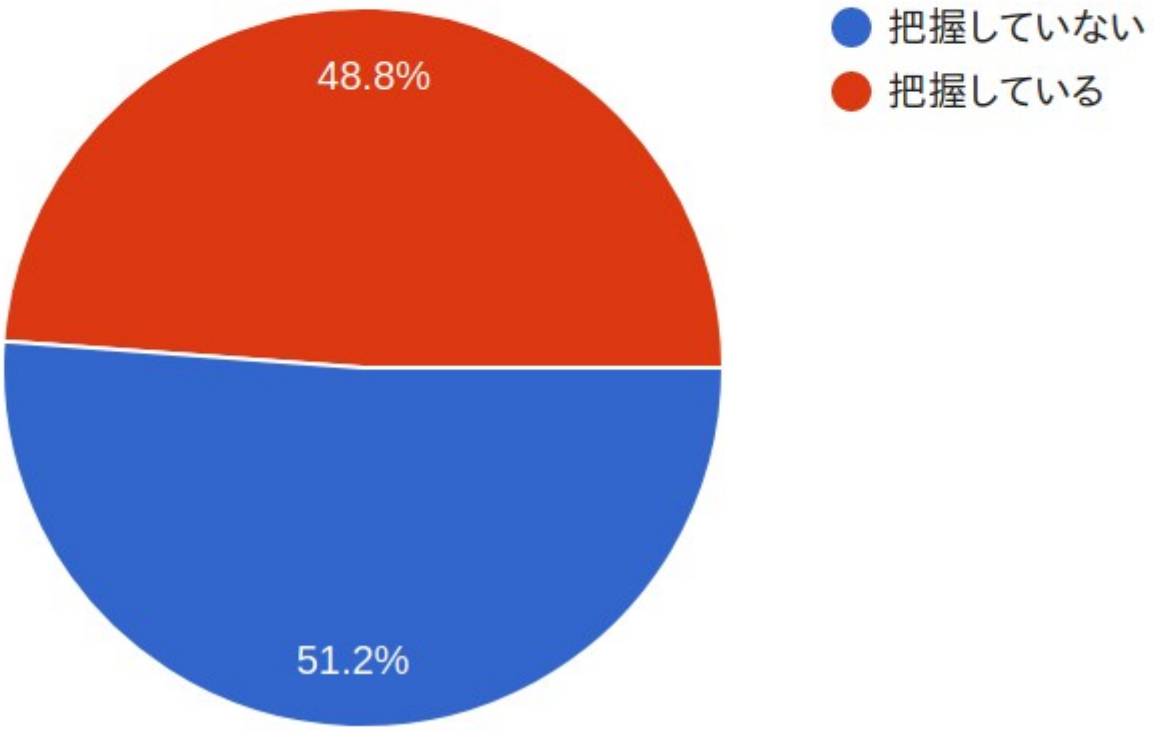
どうやって知ったか

- SNS(Twitter、Facebook等)(13回答)
- Cisco、ベンダーから連絡(10回答)
- 社内からの情報共有(2回答)
- 顧客からの情報共有

(自己証明書の管理って悩ましいよね)

今回の問題に限らず管理してるネットワーク機器およびサーバーが自己証明書を使ってるか把握していますか？

43 件の回答



どうやって管理しているか

- 理由があって管理していない
  - 管理機器、ネットワーク機器では自己証明書を利用していない(2回答)
  - 有効期間が極めて長い(10年とか)ものが多いので大丈夫だろうと管理していなかった
- ツールを利用
  - カレンダーとチケット
  - エクセル
  - gitlabにissueを登録
- メーカーからの通知に頼っている

(有用な技術コメント集)

有用な技術コメント 1

- 把握しているだけで管理はできていないが、5年後に切れそうなものやサーバ側のOSを上げるとハッシュアルゴリズムが非対応になってネットワーク機器側が死ぬとか起こるので対応は計画している
  - ovs-pkiのハッシュアルゴリズムがUbuntu14.04だとMD5だが、Ubuntu16.04でSHA512になったため、Ubuntuのバージョン上げるタイミングで証明書も更新しないといけない

(ゆやりんさんからの情報)

有用な技術コメント 2

- 証明書の期限を長くする対応を取ろうとしているが2050年前後で日付のフォーマットが変わるので2050年以降にexpireする証明書を作ると古い機器やOSで認識できなくて死ぬことがあるので気を付けてください
  - RFC5280 says “CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime”

(ゆやりんさんからの情報)

有用な技術コメント 3

- 自己証明じゃなく正規のサーバ証明がうまく入らない機材がある。具体的には、中間証明が入らず自己証明になったり、CT証明に対応できず自己証明になる機材がある。
  - 某JUNOSのバグだったので報告したら治った

(相川@日大さんからの情報)

(今回は避難訓練になったのかな？)

怒りのコメント

- Ciscoのやる気がなさすぎてコメントすると汚い言葉をいっぱい並べてしまいそう

達観したコメント

- 人生そんなもんかと :ok: :aruaru:

  by 大久保@さくらインターネットさん

(最後のスライド)