いかにして我々は7/19の史上最大規模の障害から復旧したのか

2025/01/24

小岩秀和(h-koiwa @ bitstar.jp)

ビットスター株式会社/(一社)LOCAL/88nite/奥野一門

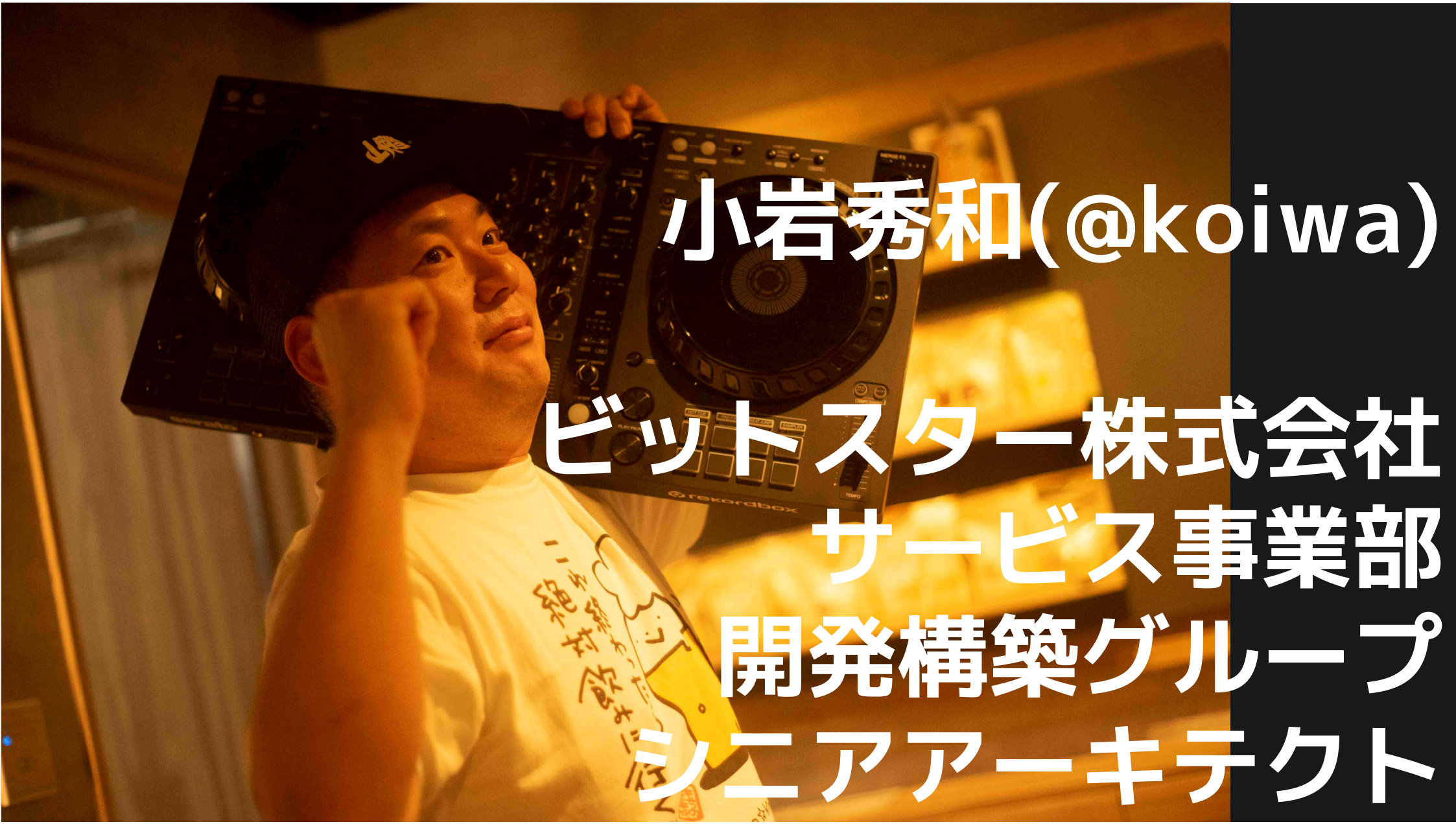
お願い

このセッションでは、
とあるセキュリティ製品について
言及しますが、その製品を貶めたり非難したりする意図は一切ありません。

発生した障害から復旧する過程で
得た学びや気付きをみなさんと共
有し議論するのが、
このセッションの目的です。

なので、SNSなどで共有されるさいはその点を踏まえてコメントしていただけると助かります。

自己紹介


小岩秀和(@koiwa)
ビットスター株式会社
サービス事業部
開発構築グループ
シニアアーキテクト

bitstar

ITで、
こまったを、よかったに。

ビットスターはITを活用して、
お客さまの事業を継続的に支援する会社です。

私たちはMSP・インフラ構築・Web制作・ソフトウェア開発を、一貫して直営でご提案・ご提供することにより、お客さまの事業課題の解決に努めています。

会社紹介

ビットスター株式会社 会社概要

商号	ビットスター株式会社
設立	2008年3月25日
所在地	札幌本社 / 〒060-0061 北海道札幌市中央区南1条西4丁目5番地1 札幌大手町ビルB1F 東京オフィス / 〒160-0023 東京都新宿区西新宿7-20-1 住友不動産西新宿ビル33F 福岡オフィス / 〒810-0042 福岡県福岡市中央区赤坂1丁目12-15赤坂門プライムビル 7F Busico.銀座 / 〒104-0061 東京都中央区銀座1-3-3 G1ビル7F Busico.梅田 / 〒530-0001 大阪府大阪市北区梅田1丁目11番4-923号 大阪駅前第4ビル9F
資本金	1,000万円
従業員数	103名
事業内容	インターネットサービス事業 各種サービスインテグレート事業 各種上記に関わるコンサルティング事業 バーチャルオフィス・シェアオフィス事業
役員	代表取締役　前田 章博 取締役　菊池敏幸 取締役　松田貴志 取締役　川村貴宏 取締役　山内耀太 取締役　瀬島大生 監査役　濱中徹 監査役　松本将司
グループ会社	さくらインターネット株式会社 クラウドネットワークス株式会社

bitstar

ビットスターの事業領域

システム開発からネットワーク配線まで、ITのこんなことできる？に応えます。

01 MSP事業

当社では、インフラ構築のご相談からソフトウェア開発、Web制作、そしてサービスローンチ後の運用サポートを幅広くご提供しております。個々にサービスをご利用して頂くのはもちろん、組み合わせでのご提供も可能です。

02 インフラ構築事業

お客さまの要望をお聞きして最適なインフラを構築いたします。
昨今、ニーズの高いクラウドでのインフラ構築も可能です。また、有人監視で24時間365日システムを見守るサポートも行います。

03 Web制作事業

PC・スマートフォンなどのWebサイトやスマートフォンアプリ、業務システムの制作実績を活かし、お客さまのご要望に応じて最適なUI/UIX設計や、インフォメーションアーキテクチャ・デザインをご提案いたします。

04 ソフトウェア開発事業

事業様々な言語とプラットフォームを使用できる幅広い知識を持ったエンジニアが、業務システム開発から消費者向けITサービス開発までお応えいたします。

bitstar

一緒にチャレンジしませんか？

ITで、こまったを、よかったに。

北の大地でスタッフ募集中

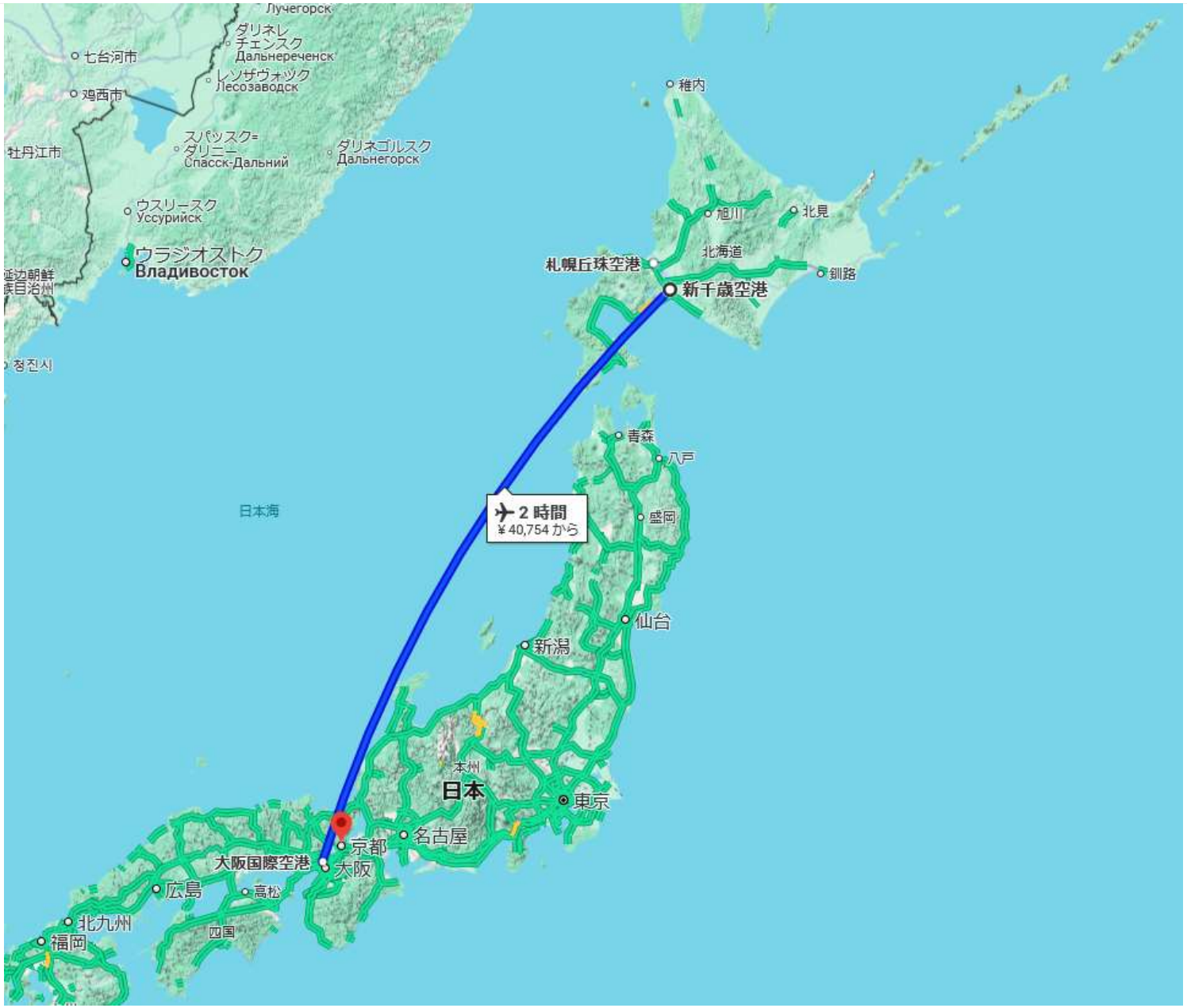
働きやすさ①
在宅勤務
対応あり

働きやすさ②
時差出勤
退勤可能

働きやすさ③
年間休日数
120日以上

働きやすさ④
副業・サイド
ビジネスOK

＋ And More! 他にもお得な制度がもりだくさん！


Лучегорск
ダリネレチェンスク
Дальнереченск
七台河市
レソザヴォツク
Лесозаводск
鸡西市
稚内
スパッスク=ダリニー
Спасск-Дальний
ダリネゴルスク
Дальнегорск
牡丹江市
旭川
北見
ウスリースク
Уссурийск
北海道
ウラジオストク
Владивосток
札幌丘珠空港
釧路
新千歳空港
청진시
青森
八戸
日本海
2 時間
¥ 40,754 から
盛岡
仙台
新潟
本州
日本
東京
名古屋
京都
大阪国際空港
大阪
広島
高松
北九州
四国
福岡

質問はできるだけ反応します

- janog-slack
  - #janog55-第3展示場b
- X(twitter)
  - #JANOG55
- mixi2
  - #JANOG55

１１３枚/３０分
議論 １５分

前提知識

題材となるシステム

弊社で構築し保守してる
お客様の基幹システム
さくらのクラウドで稼働
Windows Serverで動作


拠点
ハウジング
ラック
ハイブリッド
接続
クラウド
サーバ


さくらのクラウド

日本企業で最も利用されている国産パブリッククラウド

さくらのクラウド
sakura cloud

ビジネス規模や成長にフィットするさくらのクラウド

低価格な料金プランと圧倒的なコストパフォーマンス

東京・北海道石狩の複数拠点に環境構築 BCP/DR対策に	✓複数リージョンにサーバー環境を作ることで災害や障害からの復旧、バックアップからの復元が可能です。さまざまなトラブルからトヨックス様の損害を最小限に抑えます。今回のように、石狩第1・東京第2ゾーンで環境構築することで低レイテンシーを実現します。
堅牢な設備、万全のセキュリティ 障害発生におけるリスクを回避	✓堅牢な設備、万全のセキュリティ管理の自社国内DCにて運用。災害が少なくDR対策にも最適な北海道と、利用者がアクセスしやすい東京からお選びいただけます。 ✓大量のホストサーバーによって構成された巨大なリソースプールを効率的に運用する仕組みが備わっています。万が一ホストサーバー上で障害が発生しても、独自のフェールオーバー機能により、他のホストサーバー上で仮想サーバーが自動復旧しサービスが継続されます。
サービス品質保証(SLA)は、月間の サーバー稼働率99.95%以上を保証	✓さくらのクラウドにおいて、サービス品質の水準を定めており、月間のサーバー稼働率が、99.95%以上であることを保証しています。
日本政府が求めるセキュリティ要件 (ISMAP)を満たしたクラウド	✓さくらのクラウドは日本政府情報システムに求められるセキュリティ基準を満たしたクラウドサーバです。政府機関が情報システムのクラウド基盤として、また、情報システム開発者などが政府機関向けに納入するシステムのクラウド基盤としてさくらのクラウドを採用することが可能となり、より安心して「さくらのクラウド」をお選びいただけます。

押さえて欲しいポイント

- IasSがメインのサービス
- 仮想サーバのコンソールにアクセス可能

はじまり

「史上最大規模」の障害引き起こしたクラウドストライク、EDRに内在したバグの正体

鈴木 慶太　日経クロステック／日経コンピュータ 、 島津 忠承　日経クロステック／日経NETWORK

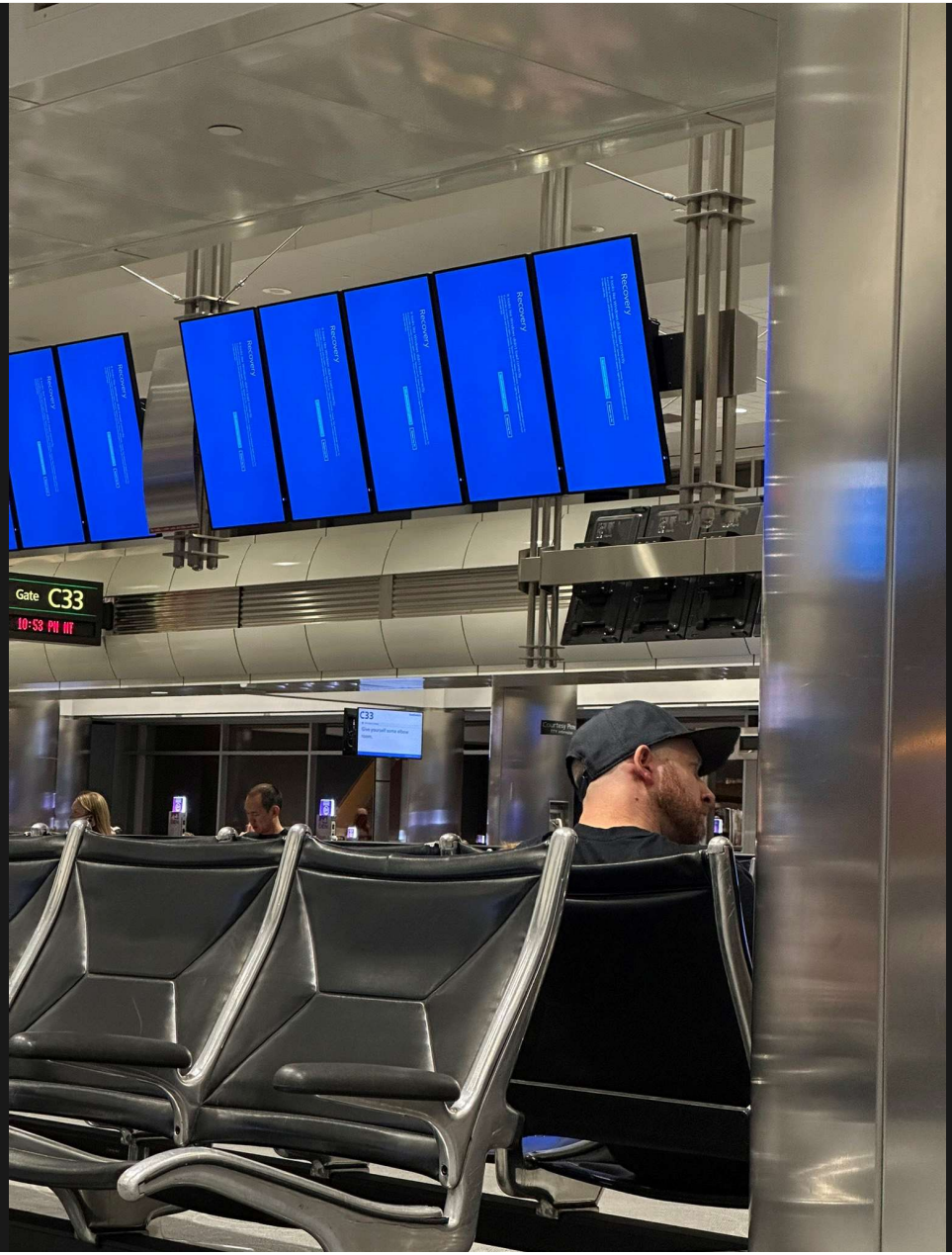
2024.08.01

有料会員限定

全3170文字

日本時間の2024年7月19日、世界各地で大規模なシステムトラブルが相次いだ。原因は米クラウドストライクのセキュリティー製品「Falcon」だった。Windowsのブルースクリーンエラーを引き起こすバグが設定ファイルに内在。同設定ファイルの配信を始めると、Windows端末が次々にダウンしていった。影響があった端末は世界で約850万台と見られ、史上最大規模の障害を招いた。

2024年7月19日午後1時ごろ（日本時間）、米マイクロソフトのOS「Windows」を搭載したコンピューターでブルースクリーンエラーが相次ぎ、世界的なシステムトラブルが勃発した。世界中の交通インフラや金融サービス、病院、政府機関、報道機関などに影響を及ぼし、「史上最大規模」のシステム障害とされる。米保険会社パラメトリックスソリューションズの推定によると、マイクロソフトを除く米フォーチュン500社の金銭的な損失は54億ドル（約8300億円）に達するという。


Recovery
Gate C33
10:53 PM HT

【空港】

19日午後1時40分ごろ、成田空港を拠点とするLCC＝格安航空会社、ジェットスター・ジャパンの国内線の搭乗手続きのシステムが使えなくなるトラブルが起き、午後5時現在、国内線のあわせて20便の欠航が決まったということです。

7/19 14:30

監視チーム 14:30

@h-koiwa.bitstar

```
:Zabbix agent on  is unreachable for 5 minutes
```

上記アラートが14:27に発生しました。

監視チーム 14:45

@h-koiwa.bitstar

```
: Zabbix agent on  is unreachable for 5 minutes
```

上記アラートが14:33-14:42に発生しました。

監視チーム 14:48

@h-koiwa.bitstar

```
Zabbix agent on  is unreachable for 5 minutes
```

上記アラートが14:48に発生しました。

1 件の返信 6ヶ月前

監視チーム 14:56

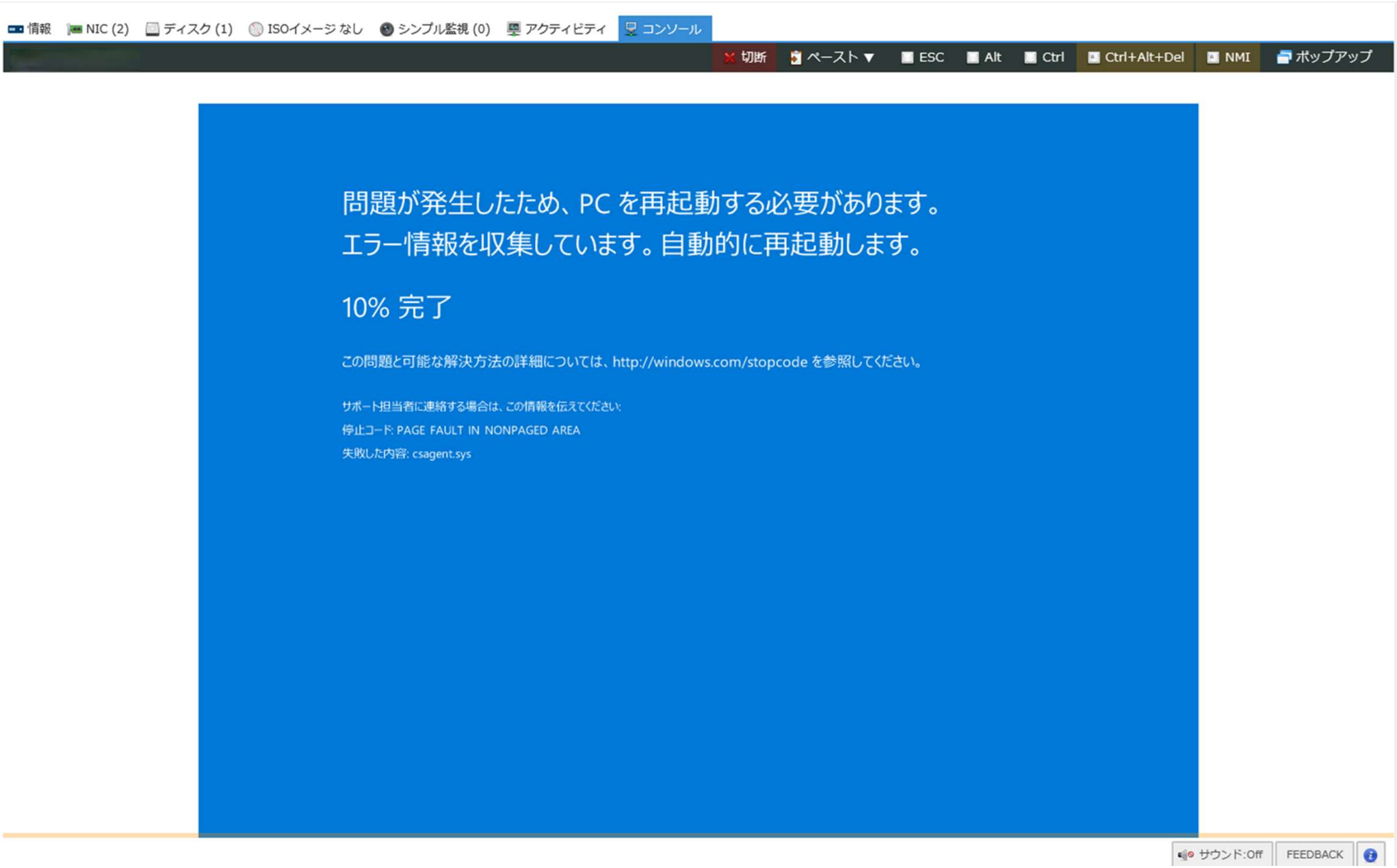
@h-koiwa.bitstar

```
Zabbix agent on  is unreachable for 5 minutes
```

上記アラートが14:54-14:55に発生しました。

なに？
なにが起きてんの？

とりあえず
適当に1台選んで
コンソール見てみる


情報
NIC (2)
ディスク (1)
ISOイメージ なし
シンプル監視 (0)
アクティビティ
コンソール
切断
ペースト ▼
ESC
Alt
Ctrl
Ctrl+Alt+Del
NMI
ポップアップ
問題が発生したため、PC を再起動する必要があります。
エラー情報を収集しています。自動的に再起動します。
10% 完了
この問題と可能な解決方法の詳細については、http://windows.com/stopcode を参照してください。
サポート担当者に連絡する場合は、この情報を伝えてください:
停止コード: PAGE FAULT IN NONPAGED AREA
失敗した内容: csagent.sys
サウンド:Off
FEEDBACK

え？
なんでセーフモード
に落ちてんの？

とりあえず再起動
セーフモードになる
の繰り返し


オプションの選択
続行
終了して Windows Server
に進みます
PC の電源を切る
デバイスの使用
USB ドライブ、ネットワーク接続、または
Windows リカバリ DVD を使います
トラブルシューティング
PC を初期状態に戻すか、詳細オプションを
表示します

1台だけ
→そのサーバの問題
複数台なので
→クラウド基盤の問題？
→障害情報は特に無し

原因判明

お客様から一報
「ワールドワイドで起きてるみたい」
「クラウドストライクが原因らしい」

クラウドストライク？

うちの保守範囲
　ネットワーク、OS、クラウド部分
　ミドルウェアはタッチしない
なので
　そいや入れ替えるって言ってたなぁ
　ぐらいの認識

とりあえず状況を確認するために、
X(twitter)で検索してみる

「cloudstrike」

と…

FF7のクラウドの
あられもない姿に
埋め尽くされる
俺のブラウザ

ニュースサイトで
情報が出始めて、
なるほど…と
状況が把握できるようになる

復旧方法

原因はわかった
だが、復旧方法がわからん

なんかこのファイルが怪しいんじゃない？　みたいな情報が出回りはじめる

BradW-CS commented on **post**

reddit

7/18/24 10:20PM PT - Hello everyone - We have widespread reports of BSODs on windows hosts, occurring on multiple sensor versions. Investigating cause. TA will be published shortly. Pinned thread.

SCOPE: EU-1, US-1, US-2 and US-GOV-1

Edit 10:36PM PT - TA posted: https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19

Edit 11:27 PM PT:

CrowdStrike Engineering has identified a content deployment related to this issue and reverted those changes.

Workaround Steps:

1. Boot Windows into Safe Mode or the Windows Recovery Environment
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
3. Locate the file matching "C-00000291*.sys", and delete it.
4. Boot the host normally.

217 upvotes 891 replies

View 891 comments

直感的には
正しそうな気がする

ただ、
再起不能にしてしまった場合、
「redditに書いてありました」
じゃ、言い訳にもならん

悶々とした時間を過ごす…

CROWDSTRIKE

[redacted]

Home

Community

Support

Environments

Legal

Tech Alert | Windows crashes related to Falcon Sensor | 2024-07-19

Favorite

Cloud: US-1 EU-1 US-2

Published Date: Jul 18, 2024

Summary

CrowdStrike is aware of reports of crashes on Windows hosts related to the Falcon Sensor.

Details

Symptoms include hosts experiencing a bugcheck\blue screen error related to the Falcon Sensor.

Current Action

CrowdStrike Engineering has identified a content deployment related to this issue and reverted those changes.

If hosts are still crashing and unable to stay online to receive the Channel File Changes, the following steps can be used to workaround this issue:

Workaround Steps:

1. Boot Windows into Safe Mode or the Windows Recovery Environment
2. Navigate to the C:\Windows\System32\drivers\CrowdStrike directory
3. Locate the file matching "C-00000291*.sys", and delete it.
4. Boot the host normally.

Latest Updates

2024-07-19 05:30 AM UTC | Tech Alert Published.
2024-07-19 06:30 AM UTC | Updated and added workaround details.

Support

Find answers and contact Support with our Support Portal

Was this helpful? Yes No

Create Case

ｷﾀ━━━━━━(°∀°)━━━━━━!!

復旧への道

この時点で
サーバの状態は2種類

1.セーフモードでログイン可能
2.再起動ループ

セーフモードで
ログイン可能

これは簡単
セーフモードでログイン後、
該当ファイルを削除して
再起動で復旧

再起動ループ

他のOSで
ディスクをマウントして
該当ファイルを削除する

LinuxOSでmount

ディスクはmount可能

しかし、
C:¥windows以下が見えない

ディスクはmount可能

しかし、
C:¥windows以下が見えない

BitLocker?

でも、普通にmountできた

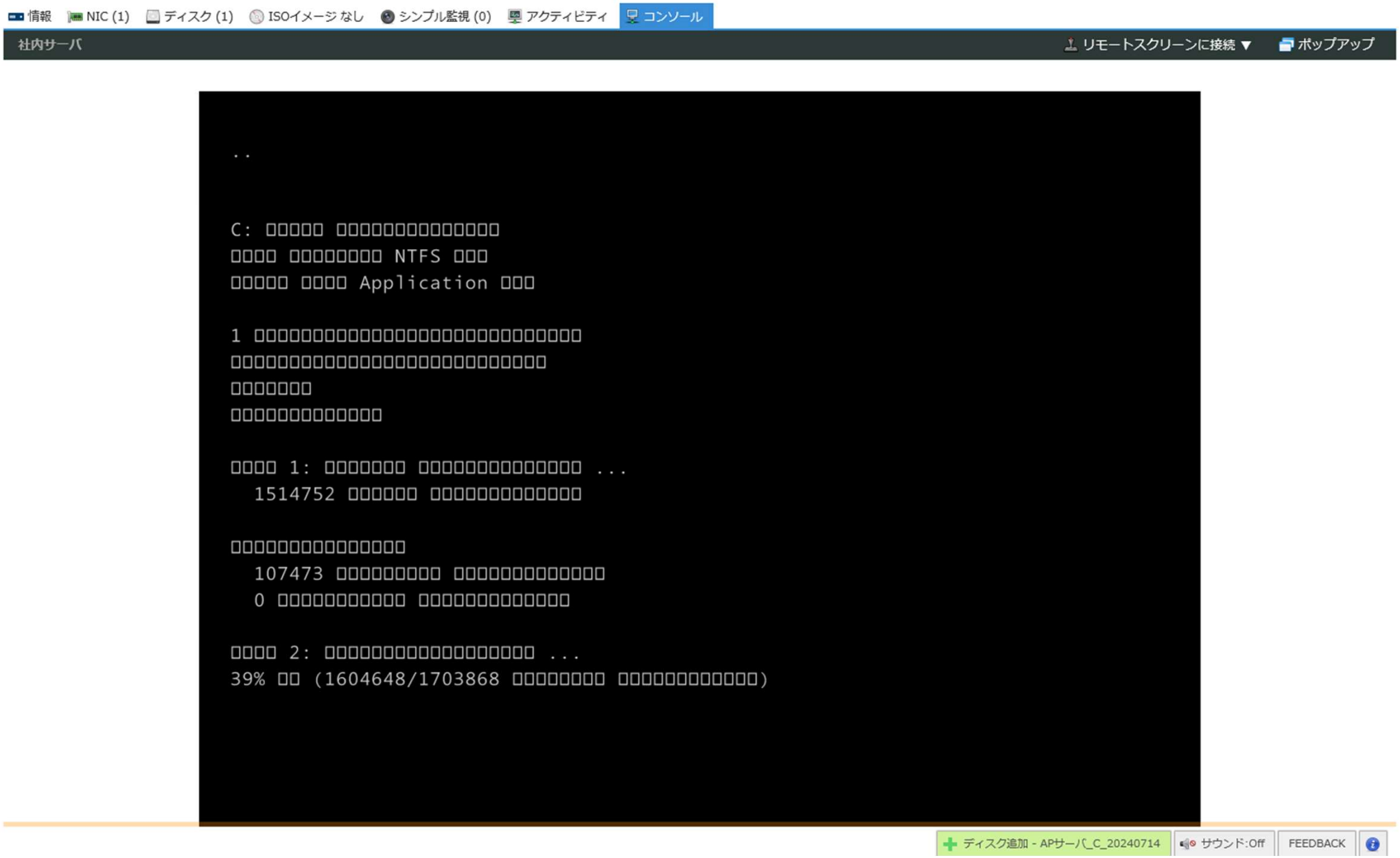
なんかそういう~~邪魔な~~機能？

深追いしてる暇はない

WindowsOSでmount

セーフモードで
起動したWindowsで
mountしてみる

やったぜ！
c:¥windows配下も見える
該当ファイルを消す
umountして
サーバに接続して起動


情報
NIC (1)
ディスク (1)
ISOイメージ なし
シンプル監視 (0)
アクティビティ
コンソール
社内サーバ
リモートスクリーンに接続
ポップアップ
..
C: □□□□□□ □□□□□□□□□□□□□□□□
□□□□□ □□□□□□□□□ NTFS □□□
□□□□□□ □□□□□ Application □□□
1 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□
□□□□□□□□□□□□□□□
□□□□□ 1: □□□□□□□□ □□□□□□□□□□□□□□□□ ...
1514752 □□□□□□□ □□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□
107473 □□□□□□□□□□ □□□□□□□□□□□□□□□□
0 □□□□□□□□□□□□□ □□□□□□□□□□□□□□□□
□□□□□ 2: □□□□□□□□□□□□□□□□□□□□ ...
39% □□ (1604648/1703868 □□□□□□□□□ □□□□□□□□□□□□□□□)
ディスク追加 - APサーバ_C_20240714
サウンド:Off
FEEDBACK

終わったわ

3. 異なるバージョンの Windows を使用して、レスキュー用の Windows インスタンスを起動します

必ず、復旧対象のEC2インスタンスのWindows Serverとは異なるバージョンのWindows Serverを作成してください。

作成手順の詳細は省略します。以下のポイントに注意してください：

- RDP接続またはSystems Manager Fleet Managerで接続できる状態であれば問題ありません。

リザルト

自然復旧：3台
セーフモードでリカバリ：5台
バックアップからリストア：2台

学んだこと

バックアップ戦略の見直し

パブリック
クラウド以前

オンプレミスサーバで仮想化基盤

潤沢なストレージ
　安価ではなく最低容量がでかい
　全部、日次で7世代

バックアップ容量が
コストに直結しない

パブリック
クラウド以降

バックアップ容量が
コストに直結する

バックアップを
取れば取るだけ金がかかる

バックアップ対象や設計が
精査される

多重化システム
→マスターは取るけど
スレーブはいらなくない？

1点障害のみを考慮
→生き残りからリカバリすればよくない？
→オンプレAD DCとか

それやると
今回の障害
だと詰む

サーバ全落ちという障害にどう備えるか

普段使わない技術との向き合い方

普段使わない技術

他OSでディスクを修正する


巨人の肩に乗る


いろんな巨人の
肩に乗ってる

乗ってる巨人

フリーソフトウェア

クラウド

サービス

隠蔽化

低レイヤが隠蔽化
されることで、
高レイヤに集中できる。

サーバーレス
FaaS

でも、サーバはある

隠蔽されている技術スタックが牙を剥く

うまく動いている間は
いいんだけど…

やっぱり
低レイヤの知識が
必要なのかも

現実を見る

ITでビジネス
経済的合理性
タイパが求められる

低レイヤの知識は必要
ただ普段は使わない

普段必要ない

→使う機会がない

→教える機会がない

高校入試の出願システム、Gmailにメール届かず…… 神奈川県、受験生に「@gmail.com以外のアドレス使って」

2024年01月16日 10時48分 公開

[岡田有花，ITmedia]

神奈川県教育委員会が2024年1月4日にリリースした、公立高校入試のインターネット出願システムで、「@gmail.com」ドメインのアドレスにシステムからのメールが届かず、受験生が出願用アカウントを作成できない問題が起きている。

15日夜時点でも解消しておらず、県教委は受験生に対して、「@gmail.com以外のメールアドレスで登録してほしい」と呼び掛けている。

必要な気はする

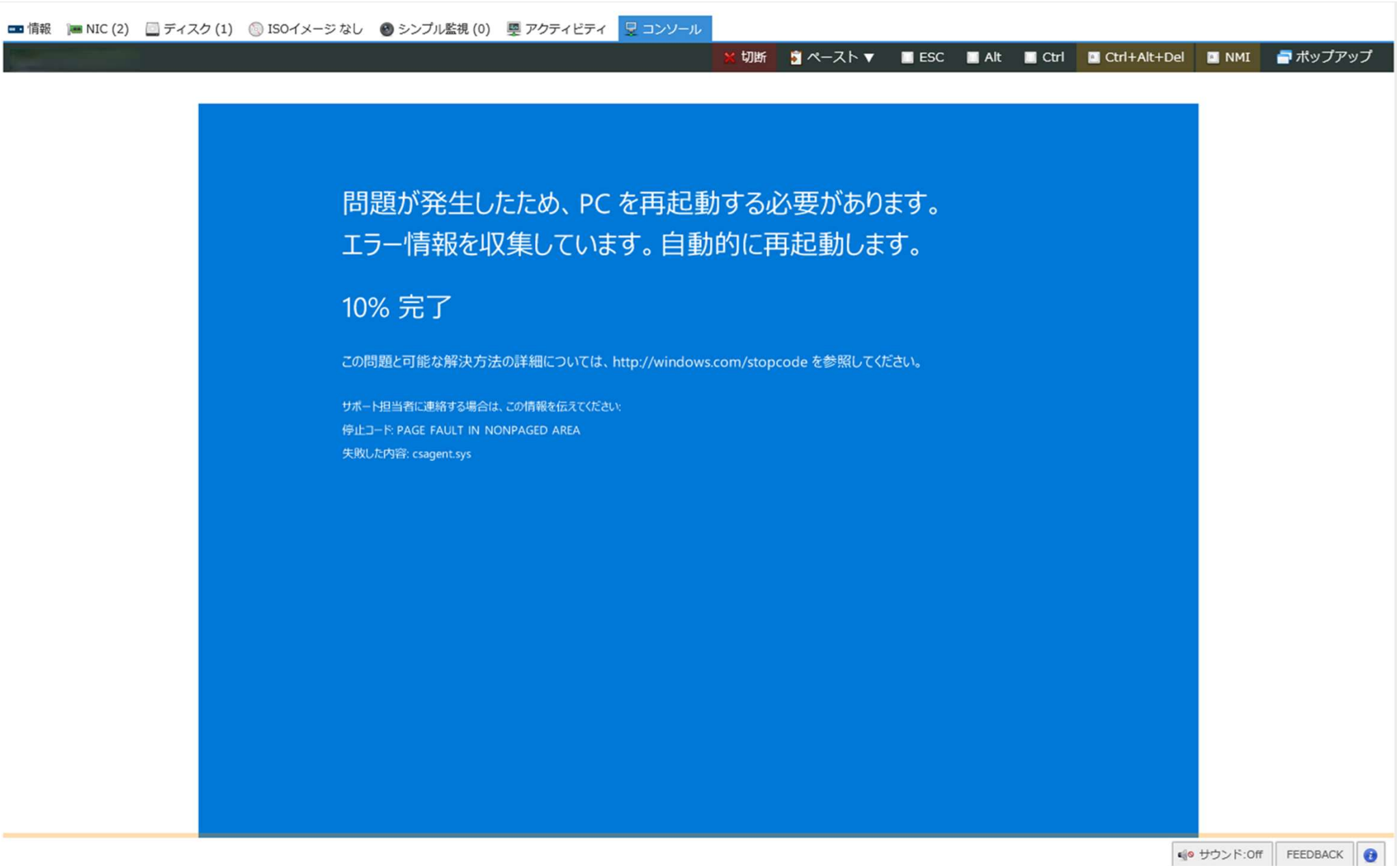
↕

普段は必要ない

さて
どうしましょうか

まとめ

7/19 14:30


情報
NIC (2)
ディスク (1)
ISOイメージ なし
シンプル監視 (0)
アクティビティ
コンソール
切断
ペースト ▼
ESC
Alt
Ctrl
Ctrl+Alt+Del
NMI
ポップアップ
問題が発生したため、PC を再起動する必要があります。
エラー情報を収集しています。自動的に再起動します。
10% 完了
この問題と可能な解決方法の詳細については、http://windows.com/stopcode を参照してください。
サポート担当者に連絡する場合は、この情報を伝えてください:
停止コード: PAGE FAULT IN NONPAGED AREA
失敗した内容: csagent.sys
サウンド:Off
FEEDBACK

原因究明

復旧への道

学んだこと

バックアップ戦略の見直し

普段使わない技術との向き合い方

議論のポイント

バックアップの話
隠蔽されている技術スタック
他、気になった点

いかにして我々は7/19の史上最大規模の障害から復旧したのか

2025/01/24

小岩秀和(h-koiwa @ bitstar.jp)

ビットスター株式会社/(一社)LOCAL/88nite/奥野一門