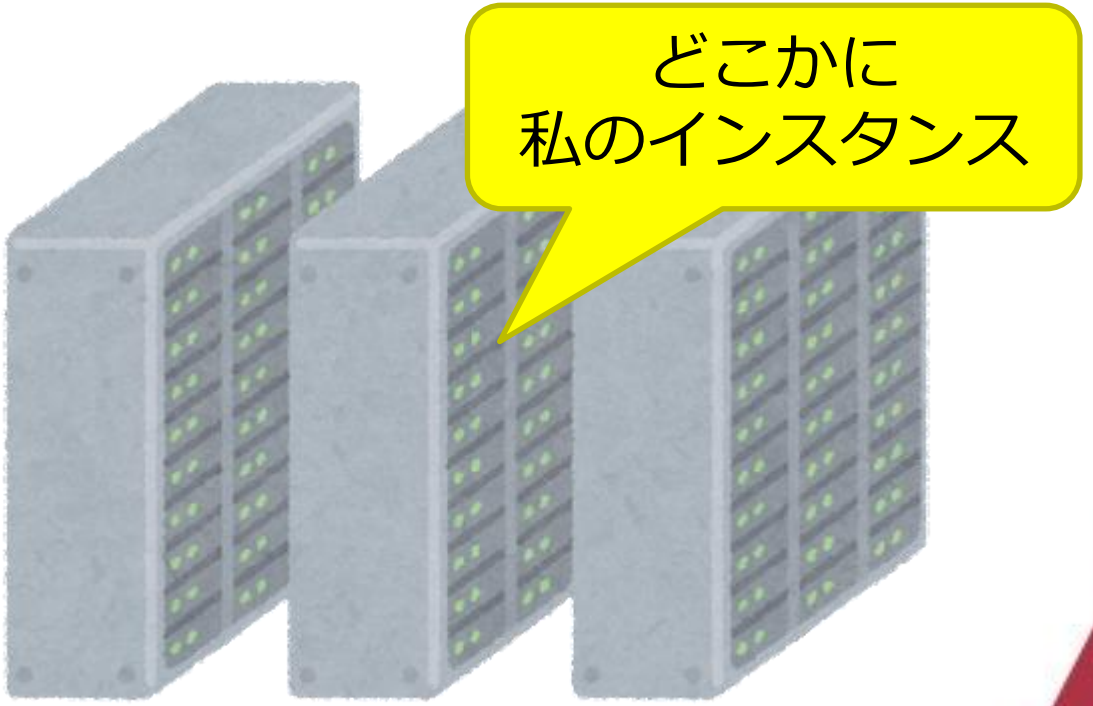
RITSUMEIKAN

クラウドフォレンジックの課題

データベース・セキュリティ・コンソーシアム 会長
立命館大学 情報理工学部　上原 哲太郎

Beyond Borders

クラウドはまさに雲をつかむようで…

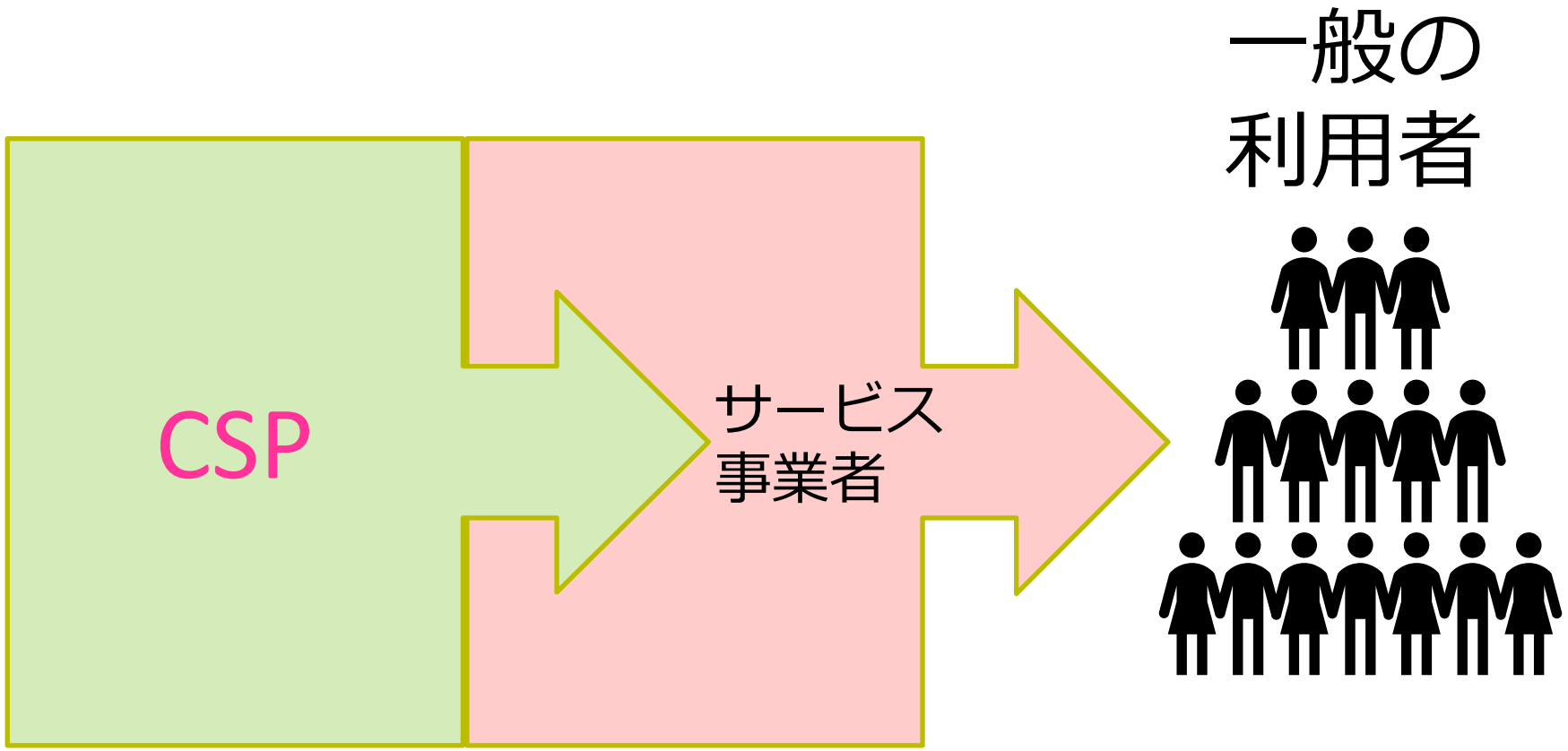


クラウドの責任共有モデル

図 1　NSA によるクラウドサービスにおける責任共有モデル

NISC クラウドを利用したシステム運用に関するガイダンス【概要】

クラウドを利用したサービスの提供



クラウドにおけるインシデントレスポンス

- クラウドを使ってサービスしている事業者は
  アクセス管理上の問題で発生したインシデントに対し
  多くの場合、自ら対応する必要がある
  - アクセス管理を行っているのは事業者側
  - 顧客がいる場合、顧客への説明責任上、情報が欲しい

- しかし基盤はCSP側の管理下にあるのでIaaS以外は
  CSP側が提供する機能を使うことになるが…

クラウドにおけるインシデントの類型

- CSPが基盤自身に起こしたインシデント
  - 基盤側の障害やオペミスに起因するインシデント
- CSPが提供する基盤へのアクセス権を奪われたことに起因するインシデント
  - AWSアカウントを窃取された等
- （IaaSの場合）VM等基盤で起きたインシデント
- クラウド上に利用者が構築したシステム上のインシデント

CSP自身が起こしたインシデント例

ファーストサーバ障害、深刻化する大規模「データ消失」
ヤフー子会社、クラウド時代の盲点を露呈（ネット事件簿）

2012年6月26日 13:27

保存

クラウドに預けていたデータが、「雲」が消えるかのごとく消失してしまった。20日17時頃、レンタルサーバー会社のファーストサーバ（大阪市）で起きた「データ消失」事故。その深刻な状況が日を追うごとに明らかになってきている。被害にあった顧客件数は5698件で、ほとんどが復旧不可能な状態。ウェブサイトやメールに加え、顧客情報やスケジュールなど多種多様なデータが失われ、業務が止まった企業からは悲痛な叫びが聞こえてくる。いったい何が起きているのか。

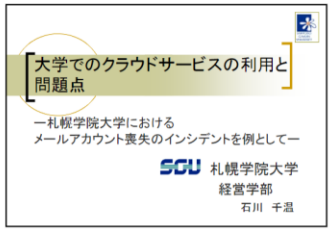
「データの消失があった5698件のお客様のうち、数百件を除く共有サーバーのデータは、残念ながらデータの復旧自体が不可能ということが分かりました。本当に申し訳なく思っております」――。

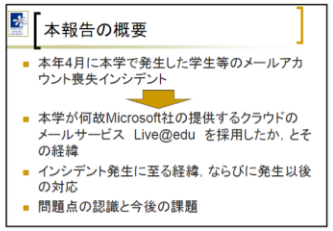
ファーストサーバ社長室の村竹昌人室長は、混乱の続く25日夜、こう語った。5万以上の顧客を抱え、うち8割が法人・官公庁関連というファーストサーバの大規模障害は、依然として被害の全容がつかめないままでいる。

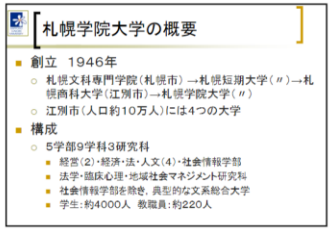
小林製薬、109シネマズ、長野電鉄、カルディコーヒーファーム、海遊館、兵庫ひまわり信用組合、薬事日報、日本新聞協会、東京都卓球連盟、静岡産業大学、大津市市民活動センター、太陽光発電協会……。

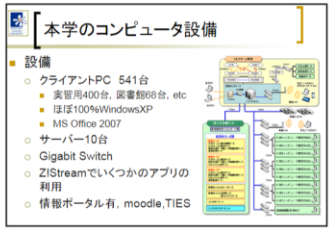
情報処理学会研究報告
IPSJ SIG Technical Report

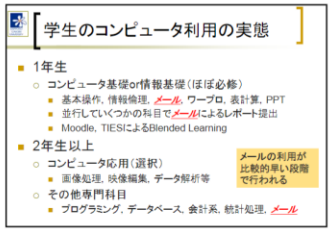
Vol.2012-EVA-39 No.8
Vol.2012-IOT-19 No.8
2012/9/28











辻伸弘の裏読みセキュリティ事件簿

韓国でランサムウエア被害、バックアップも暗号化された
辻 伸弘 ソフトバンク・テクノロジー

2017.07.26

PR
オンプレミス／クラウドの溝を超える 近未来に実現する「双方向クラウド戦略」
IT／製造／建設分野の製品・サービス選択支援情報サイト：日経クロステックActive

2017年6月10日、韓国のレンタルサーバー事業者「NAYANA」の利用者向け掲示板に、衝撃的な告知が掲載されました。同社が貸し出していた全サーバーがランサムウエアに感染し、利用者のデータが使えなくなったというものです（図1）。同社のサービスを利用する企業は数千社ありました。報道によれば、通販サイトによく使われていたそうです。

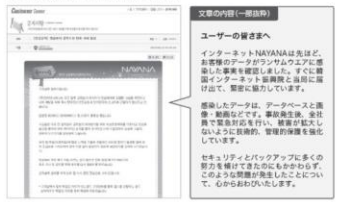


図1●ランサムウエアの被害に遭った韓国レンタルサーバー「NAYANA」
NAYANAは2017年6月10日、同社が運用するすべてのレンタルサーバーがランサムウエアに感染したことを利用者に明らかにした。データをバックアップしていたが、バックアップを使った復旧ができないといった内容が含まれる。
[画像のクリックで拡大表示]

ニュース

日本電子計算の自治体クラウドで障害、アップデート中に「想定外の事象が発生」
大豆生田 崇志 日経クロステック／日経コンピュータ

2020.06.01

PR
オンプレミス／クラウドの溝を超える 近未来に実現する「双方向クラウド戦略」
IT／製造／建設分野の製品・サービス選択支援情報サイト：日経クロステックActive

日本電子計算（JIP）は2020年6月1日、同社が提供する自治体向けIaaS「Jip-Base」で5月31日未明からシステム障害が発生していたと日経クロステックの取材に対して明らかにした。6月1日午前4時30分に復旧したという。一部の自治体ではそれ以降の時間もメールを送受信できないといった症状が出ていたが、同日昼までに解消したとしている。

JIPによれば、5月31日にストレージ機器のコントローラーのファームウエアのバグを修正するアップデートを実施。そのとき、「想定外の事象が発生した」（広報）という。同社は想定外の事象に対応したうえで、予定していたファームウエアのアップデートを最後まで行ったとしている。

ストレージに構築している仮想OSなどのクラウドサービスを利用している自治体の業務システムに影響が出たようだ。Jip-Baseは2019年12月にもストレージ機器のファームウエアの不具合が原因となって、50自治体のシステムが一斉にダウンして住民票が発行できなくなり、データの一部を消失するというトラブルが発生した。同社の広報担当者は、今回のトラブルの原因は前回とは異なるとしている。

関連記事：自治体クラウド、復旧難航 障害で15%のデータが消失

この記事の目次へ戻る

2017年 NAYANA事件

2020年 JIP-BASE事件

2012年ファーストサーバ事件

2012年 札幌学院大事件

JIP-BASE事案の教訓

動かないコンピュータ

＋ 特集をフォロー

「動かないコンピュータ」緊急版、自治体クラウド大規模障害の深層

日本電子計算

松浦 龍夫　日経コンピュータ

2019.12.18

全2685文字

PR
オンプレミス／クラウドの溝を超える　近未来に実現する「双方向クラウド戦略」
IT／製造／建設分野の製品・サービス選択支援情報サイト：日経クロステックActive

2019年12月4日に日本電子計算の自治体向けクラウドが停止した。47自治体などのシステムが一斉にダウンし、業務や住民サービスに影響が出た。ストレージ機器のファームウエア不具合が直接の原因だが、バックアップ機能にも問題があり15%のデータがクラウド上で消失。自治体システムは全面復旧の見通しが付いていない。

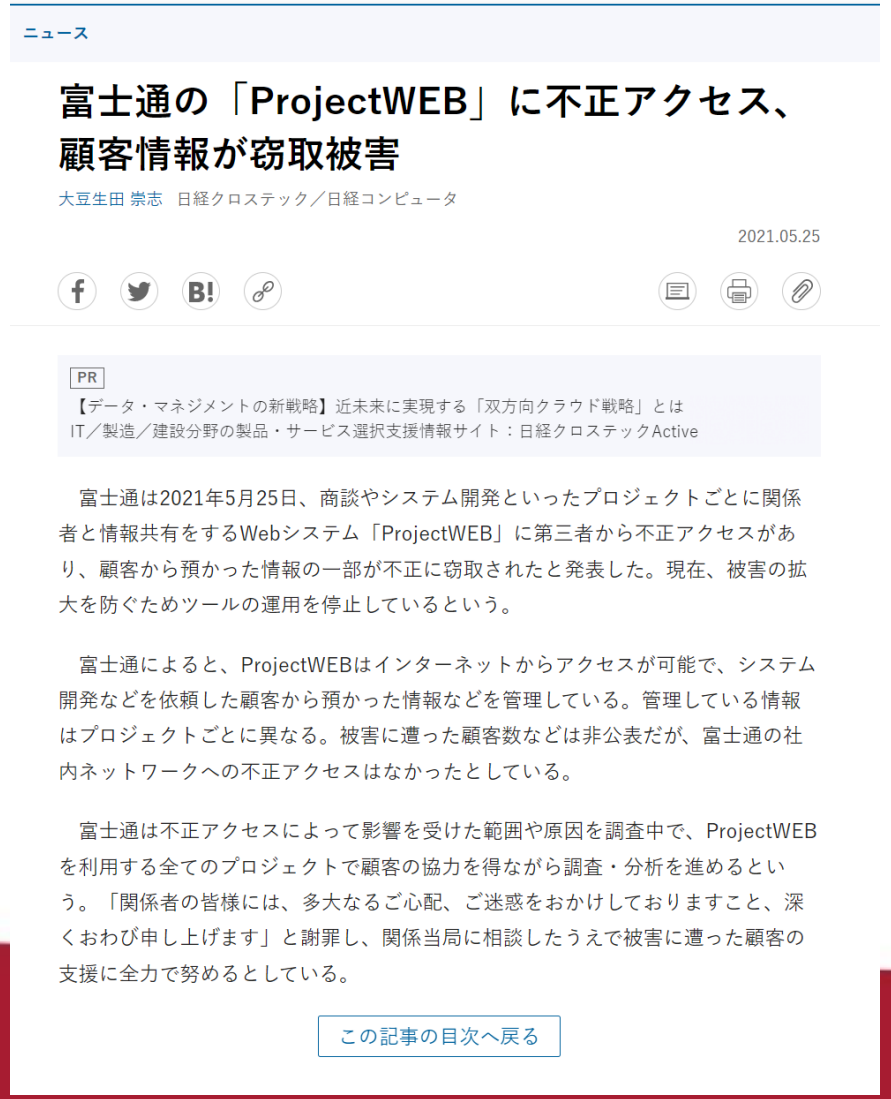
「あれ、戸籍証明を出すシステムにつながらない」。東京都中野区役所の職員が異変に気づいたのは2019年12月4日午前11時ごろ。区で使う20のシステムが停止し、戸籍関連の証明書発行業務や区のWebサイトの更新・公開、電子メールを使った外部とのやり取りなどができなくなった。

- 直接の原因は
  ストレージの障害
- しかしCSPであるJIPの
  バックアップにも問題
  - 実は動いていなかった問題
- 結果的にデータ復旧
  できなかったものも

CSP自身のインシデントへの対応の課題

- CSP自身が復旧対応の最中にある時に
  なかなか情報が出てこない
  - 利用者での影響範囲の特定など
    - その根拠となるログなど
- ログを始めとする証拠はCSP自身の手の中にあり
  取得プロセスも含めて利用者から不透明
  - 例え提供を受けられたとしても法的根拠がしっかりしている
    ＝Forensically Soundかどうかがわかりにくい

CSPが提供する基盤へのアクセス権が奪われたことに起因するインシデント



ニュース

富士通の「ProjectWEB」に不正アクセス、顧客情報が窃取被害

大豆生田 崇志　日経クロステック／日経コンピュータ

2021.05.25

PR
【データ・マネジメントの新戦略】近未来に実現する「双方向クラウド戦略」とは
IT／製造／建設分野の製品・サービス選択支援情報サイト：日経クロステックActive

富士通は2021年5月25日、商談やシステム開発といったプロジェクトごとに関係者と情報共有をするWebシステム「ProjectWEB」に第三者から不正アクセスがあり、顧客から預かった情報の一部が不正に窃取されたと発表した。現在、被害の拡大を防ぐためツールの運用を停止しているという。

富士通によると、ProjectWEBはインターネットからアクセスが可能で、システム開発などを依頼した顧客から預かった情報などを管理している。管理している情報はプロジェクトごとに異なる。被害に遭った顧客数などは非公表だが、富士通の社内ネットワークへの不正アクセスはなかったとしている。

富士通は不正アクセスによって影響を受けた範囲や原因を調査中で、ProjectWEBを利用する全てのプロジェクトで顧客の協力を得ながら調査・分析を進めるという。「関係者の皆様には、多大なるご心配、ご迷惑をおかけしておりますこと、深くおわび申し上げます」と謝罪し、関係当局に相談したうえで被害に遭った顧客の支援に全力で努めるとしている。

この記事の目次へ戻る

- 一部テナントのアクセス権が奪われていたことに起因してインシデント発生？？
- フォレンジック対応機能が実装されていたかは不明

AWSならCloudTrail

- アカウントの
利用状況
各サービスの
使用状況の
ログが取れるので
これから
証拠保全が可能

CSP上のVM等におけるインシデント

- 仮想化されているとはいえ完全に利用者の管理下のシステムになるのでインシデント対応は楽
- ただし「事前に備えておく必要がある」
  - オンプレのシステムやデータセンターと同じログをどのように取るかあらかじめ決める必要

- CSPによってはVM等へのアクセスログを基盤側で収集保全できる場合もある

AWSのVPCフローログ

CSP上に構築したサービスで起きたインシデントの場合

2020-12-28

Salesforceの設定不備に起因した外部からのアクセス事案についてまとめてみた

意図せぬ公開　情報漏えい

2020年12月25日、セールスフォースドットコムは一部製品、または機能を利用するユーザーにおいて、Salesforce上の組織の一部情報が第三者より閲覧できる事象が発生していると案内を掲載しました。また、12月に入り外部への情報流出の可能性を発表した楽天、PayPayがこの影響を受けたユーザーに含まれていたことが報じられています。ここでは関連する情報をまとめます。

設定不備で第三者からの情報閲覧事象が発生

セールスフォース・ドットコムからのお知らせ

www.salesforce.com 266 users

www.salesforce.com

セールスフォースドットコムが公開したリリースをまとめると以下の通り。

- 影響を受ける対象機能、製品はExperience Cloud（旧 Community Cloud）、Salesforceサイト、Site.com。
- 既に当該機能、製品利用組織において第三者による閲覧行為が発生している。
- 脆弱性起因の問題で生じた事象ではなく、ゲストユーザーに対する情報共有に関する設定が適切に行われていない場合に起こる。
- ユーザーに対し、メール、コミュニティグループ、自社社員を通じて連絡を行っている。

またユーザーに対しゲストユーザーに対する共有設定の確認を呼び掛けており、以下のベストプラクティスを公開している。

- ゲストユーザセキュリティポリシーのベストプラクティス

12月28日、29日に更新を行い以下の内容を追記している。

- 設定確認方法が不明な場合は担当営業、サポートまで問合せしてほしいこと。
- 2016年の製品アップデートに際し、ゲストユーザー権限の共有関係設定に変更があったという事実はないこと。
- ゲストユーザーの共有設定が顧客の要件に遵っているかは各自確認を行う必要があること。

- **PaaSにおけるインシデント対応の難しさを実感した事案**
  - **CSP側で提供されるツールがインシデントレスポンスに不十分でタイムリーに対応が取れない**
- **NISCからの注意喚起につながる**

備えあれば憂いなし

- CSPの基盤側で起きるインシデントへの事前準備
  - そもそもCSPが提供される機能を知っておく
  - 緊急時のログ保存などフォレンジックに必要な証拠保全の体制を事前に整えておく
- CSPで提供しているサービス側で起きるインシデントへの事前準備
  - SaaS/PaaSならCSP提供機能を知る・契約する
  - PaaS/IaaSでは自らもログ保全機能等を実装しておく

残っている課題

- CSPに頼るしかない機能の信頼性は？
  - 保全した証拠へのタイムスタンプ等　第三者の介在は？
- 米国ではOKでも我が国のニーズには応えてくれるか?
  - 「記録命令付き差押」
  - 越境問題
- そもそもCSPごとにバラバラで利用者は大変
  - アーキテクチャ（とその背後の思想）の違い
  - ターミノロジー（用語）の違い