これにより、例えば不要になった検証用仮想マシンが残っていることを見つけたり、事業とシステム、仮想リソースを紐づけして、仮想リソースの管理者が誰であるかということも可視化できます。

さらに、未申告で使われていたり、放置されているAWSやAzureのアカウントを検知して、利用者にサービスへの登録を促したり、アカウントの削除を依頼することで、セキュリティリスクを低減することもできます。

自動セキュリティ診断で、システムの脆弱性を定期的に把握

万が一利用している仮想リソースにセキュリティリスクが見つかった場合は、優先度をつけて対応を行うことが重要となります。クラウドワークロードセキュリティサービスは、仮想リソース上で稼働する各システムのセキュリティ設定不備、脆弱性診断を自動で定期的に実施します。その結果をもとに、事前に登録した事業の重要性を加味したうえで、セキュリティリスクの判断やBCP対策時の復旧などを優先度付けし、是正を支援できる点が大きな特長です。視覚的に対策の優先順位がわかるようにデザインされているため、リスクの大きさや発生ポイントも容易に把握できます。

このように、クラウドワークロードセキュリティサービスによってクラウド環境上の仮想リソース全体を可視化し、一括での監査・管理を実現することで、存在が把握・管理できていなかったシステムも含め、設定ミスによるセキュリティ事故を未然に防ぎ、万が一の際も事業情報や担当者が一目でわかるので、効率的に対応することができます。

IaaS/PaaS環境の導入・管理・運用でお悩みの管理者の方はぜひ、日立ソリューションズにご相談ください。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/column/shion/vol14/

C20S-02-00 | 2021.04

HITACHI
Inspire the Next

IT探偵 しおんが解決！ 企業潜入調査物語

AWS、AzureなどIaaS/PaaS環境を安全かつ効率的に運用するコツとは

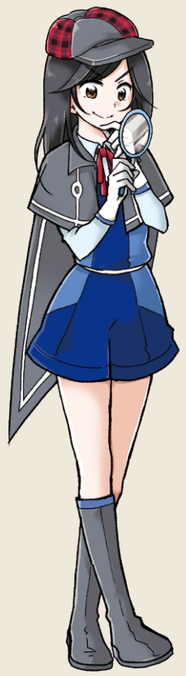
プロローグ

都内某所に、ITを駆使して企業の悩みを解決するという、特別な探偵事務所がある。そこで働くエリートIT探偵の「伊野部しおん」は、企業が悩むセキュリティや業務効率化の課題を次々と調査・解決していく。

AWS：Amazon Web Services

伊野部 しおん（いのべ）

IT探偵事務所に勤めるエリート探偵。3年前までは某企業のスーパーエンジニアだったらしい。依頼先の関係者に変装をしてITの課題を探し出して解決していく変装調査型の仕事を得意とする。



登場人物

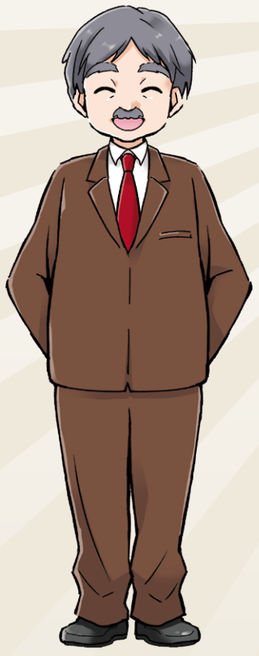
無地矢 由奈（むちや ゆな）

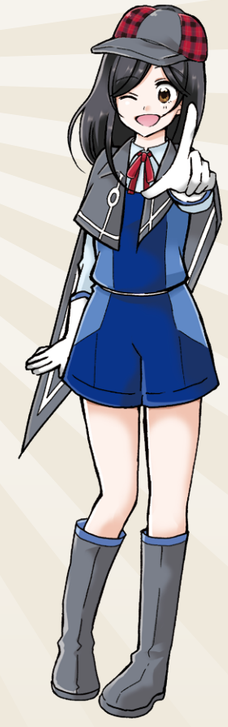
▽□社 情報セキュリティ部課長。敏腕SEで日々真面目に業務に取り組んでいるが、部長の無茶振りに振り回されることもしばしば。眼鏡のフレーム集めに凝っていて毎日違うフレームを着けているが周りには気付かれない。

曾柳 好男（そりゅう よしお）

IT探偵事務所所長兼取締役を務める社長。さまざまな企業に監査などの内部調査を依頼され、しおんを送り込んでは企業課題を解決させている。

AWS、AzureなどIaaS/PaaS環境を
安全かつ効率的に運用するコツとは





1T探偵しおんが解決!

IaaS/PaaSといったクラウド環境は導入の容易さ、運用のしやすさなどから、近年、利用する企業が増えつつあります。
その一方で、これまで社内の情報システムを統括してきた情報システム部門の手から離れて、事業部門が直接クラウド環境を契約し、運用しているという事例も増えてきています。ITガバナンスの観点からいうと、情報システム部門のあずかり知らないところで、クラウド環境が運用されることとなり、セキュリティリスクが増大することになってしまいます。
日立ソリューションズが提供する「クラウドワークロードセキュリティサービス」は企業で利用されているクラウド環境上の仮想リソースと仮想リソースのセキュリティ設定の管理を一括して行うことを実現するサービスです。仮想リソースの利用状況の可視化、事業や部署別での管理、セキュリティ診断、未申告アカウントの検知など、仮想リソース全体に対して情報システム部門が一括して管理できる環境を提供します。

大手のIaaS/PaaSだからといって何もしなければ安全とは言えない

DX（デジタルトランスフォーメーション）の推進や、ITを軸とした新規事業立ち上げなどに、ハードウェアの調達が不要でITリソースをスピーディーに柔軟に使うことができるクラウド環境の利用は効率的なソリューションです。その導入のしやすさから、事業部門が独自のサービスやシステムを構築するために契約して運用するという例も増えてきています。

ところが、一般的に全社的なITガバナンスを統括し、セキュリティマネジメントを行う情報システム部門から見れば、このように部門独自に使われるクラウド環境は、自分たちの管理の外側となってしまうため、管理を行うことができません。

特にセキュリティマネジメントの観点で言えば、AWS*1やAzureといった大手のクラウドサービスでも、適切なセキュリティ対策を実施しない限りセキュリティ事故が起こる可能性は高いままとなってしまいます。

例えば、クラウド環境のアカウント管理がしっかり行われていなかったことにより、インスタンスが仮想通貨の計算に使われていたとか、検証環境のセキュリティ設定の甘さから、クラウド上の仮想マシンに侵入され、サイバー攻撃の踏み台にされてしまうといったことが起こりうるわけです。

したがって、大手のクラウドサービスだからといって、安心することなくしっかり情報システム部門が目を光らせておく必要があります。
このようにクラウド環境上の仮想リソースのセキュリティ設定の状態を監視して管理を行うことをCSPM*2と呼びます。

*1 AWS：Amazon Web Services　*2 Cloud Security Posture Management：クラウドセキュリティ態勢管理

安全にIaaS/PaaS環境を利用するために仮想リソースの可視化は重要

先に述べたような、セキュリティ設定の甘さによるセキュリティ事故の発生を防止するために重要となるのが、仮想リソースの可視化です。

社内で部門ごとにIaaS/PaaS環境が乱立してしまうと、情報システム部門がお目付け役としてそれらを監視・管理することは困難と言えるでしょう。

しかしそのような状態では、各リソースのセキュリティ設定に問題がないかの確認を十分に行うことができません。社内で利用している仮想リソースに対し、セキュリティを確保するためにも、まずは仮想リソースの可視化が必須といっても過言ではありません。

社内で使われるIaaS/PaaS環境の仮想リソースを一括管理する

今まで見てきたように、多数のIaaS/PaaS環境を企業内で効率的、かつ安全に運用していくには、情報システム部門によってこれらの仮想リソースやセキュリティの設定状況を一括して管理し、セキュリティ課題を解決していくことが重要と言えます。

日立ソリューションズが提供する「クラウドワークロードセキュリティサービス」は、AWSやAzureといったIaaS/PaaS環境の効率的かつ安全な活用を実現するサービスです。

クラウドワークロードセキュリティサービスに各部門が利用しているクラウドサービスのアカウントや事業情報を登録することで、それぞれのIaaS/PaaS環境の仮想リソースの状態を把握、事業や部門ごとに使用している仮想リソースの管理を行うことはもちろんのこと、仮想リソースで稼動しているシステム単位での監査や棚卸も行うことができます。