



夢ある未来を、共に創る。

# なぜコンテナ活用が難しいのか？ CloudNative化の課題と処方箋 「Sysdig Secure DevOps Platform」のご紹介

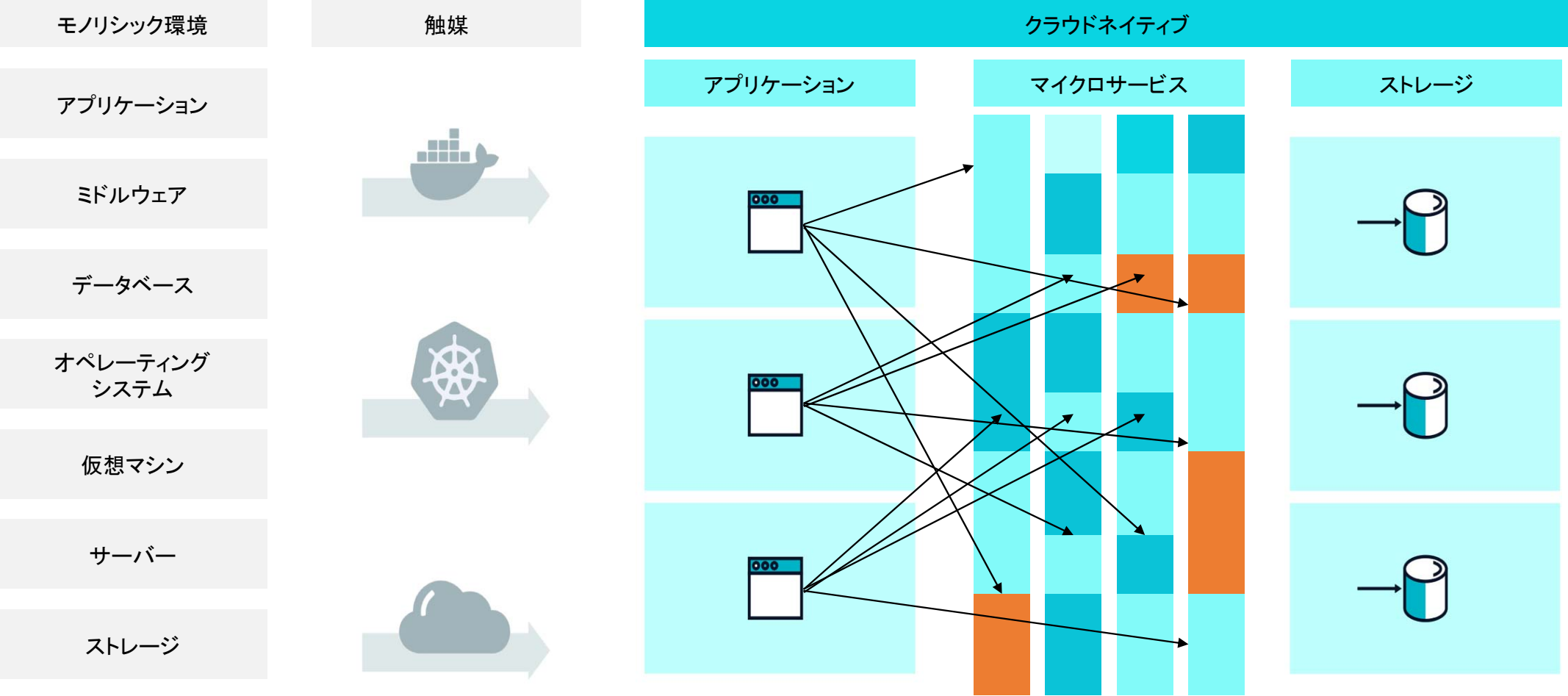
---

SCSK株式会社

ITエンジニアリング事業本部

ミドルウェア第二部

# アプリケーションアーキテクチャの変化



## コンテナ運用には、アーキテクチャの複雑化に起因した課題が存在

### コンテナ



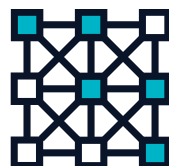
コンテナは従来のツールでみると複雑であり  
言うなれば、ブラックボックスです。

どのように中身を把握？



可視化

### マイクロサービス



大規模で分散したWebコンテナとサービスは、  
複雑でエフェメラル（短命）です。

どのように管理？



障害検知



解析

### マルチクラウド



クラウドやデータセンター間や内部でアプリケー  
ションのモニタリングと保護が必要です。

どのように行うのか？



セキュリティ

# NISTによる「コンテナ、5つのリスク」

2017年9月、アメリカ国立標準技術研究所（NIST）は、特別刊行物（SP）800-190、アプリケーションコンテナセキュリティガイドをリリース

| リスク      | 具体例（一部）                                                                            |
|----------|------------------------------------------------------------------------------------|
| イメージ     | コンテナイメージに潜む脆弱性、アクセス制御など設定の不備<br>暗号化せずに保存されるシークレット情報、信頼されないコンテナイメージの利用 など           |
| レジストリ    | コンテナイメージを配布するレジストリへの安全でない接続<br>レジストリ上での脆弱性の残ったイメージの配布、不十分な認証とアクセス制御の不備             |
| オーケストレータ | 無制限の特権アクセス、権限のない者によるアクセス、コンテナ内部トラフィックの不十分な分離<br>機密情報を扱うワークロードの混在、オーケストレーターのノードの信頼性 |
| コンテナ     | ランタイムソフトウェアに潜む脆弱性、各コンテナからの無制限なネットワークアクセス<br>信頼できないコンテナのランタイム設定、アプリケーションの脆弱性        |
| ホストOS    | カーネルを共有するリスク、OSコンポーネントの脆弱性、不適切なユーザーアクセス権限<br>ファイルシステムの書き換え                         |

# Sysdig (シスディグ) とは



## ☑ コンテナ環境のモニタリング & セキュリティ プラットフォーム

- ・Wiresharkの創作者によって開発

- ・OSのシステムコールを可視化する特許技術により、コンテナ内部やコンテナ間の通信状況を完全にモニタリング/視覚化

- ・コンテナに潜む脆弱性の発見や、不正アクセス・サイバー攻撃などの異常検知、コマンドの実行履歴をすべて記録

➡ フルフォレンジックによるトラブルシューティングを実現

## ☑ SCSKが国内総販売代理店（ディストリビューター）

# Sysdig会社概要



ロリス ディオニアニ

Wiresharkの共同創作者



## SYSDIG OPEN CORE

- オープンソースがルーツ
- 2013年に発足
- 1,000万以上のダウンロード数



## CNCF CONTRIBUTOR

Donator of Sysdig Falco, Run-time security project. Creator of Sysdig Inspect.

# 300+

お客様

# \$200M+

## CAPITAL RAISED

From Accel, Bain,  
Insight Ventures



パートナーエコシステム OpenShift,  
Docker,  
Kubernetes, AWS...

**Sysdig Wins Red Hat North American Partner Award !!** on April 23, 2020

<https://sysdig.com/press-releases/sysdig-wins-red-hat-north-american-partner-award/>



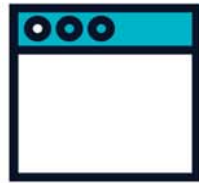
# アプローチ：コンテナ運用の課題

## ◇ カーネルは決して嘘をつかない

ノードに対しコンテナ形式でデプロイされたSysdigエージェントがホストのカーネルにアクセス  
Linuxのシステムコールを採取し可視化



コンテナ



アプリケーション



マイクロサービス



ファイル



ホスト



ホスト / OS カーネル

## オープンコアで構築されたソリューション

### Sysdig Secure DevOps Platform

Sysdig モニター

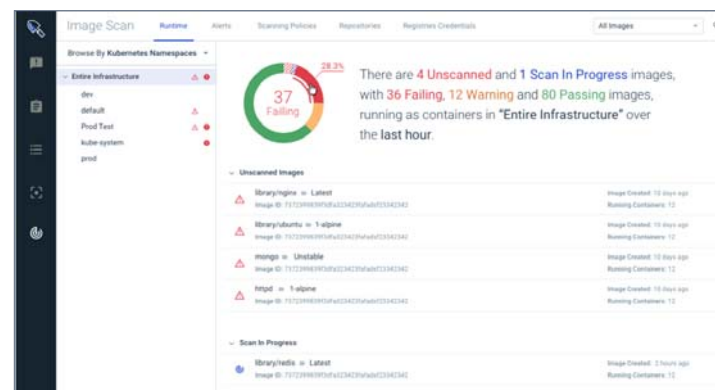


PROMETHEUS



SYSDIG INSPECT

Sysdig セキュア



FALCO



ANCHORE





# 300社以上のお客様



2020 Red Hat Innovation Awards winners!!

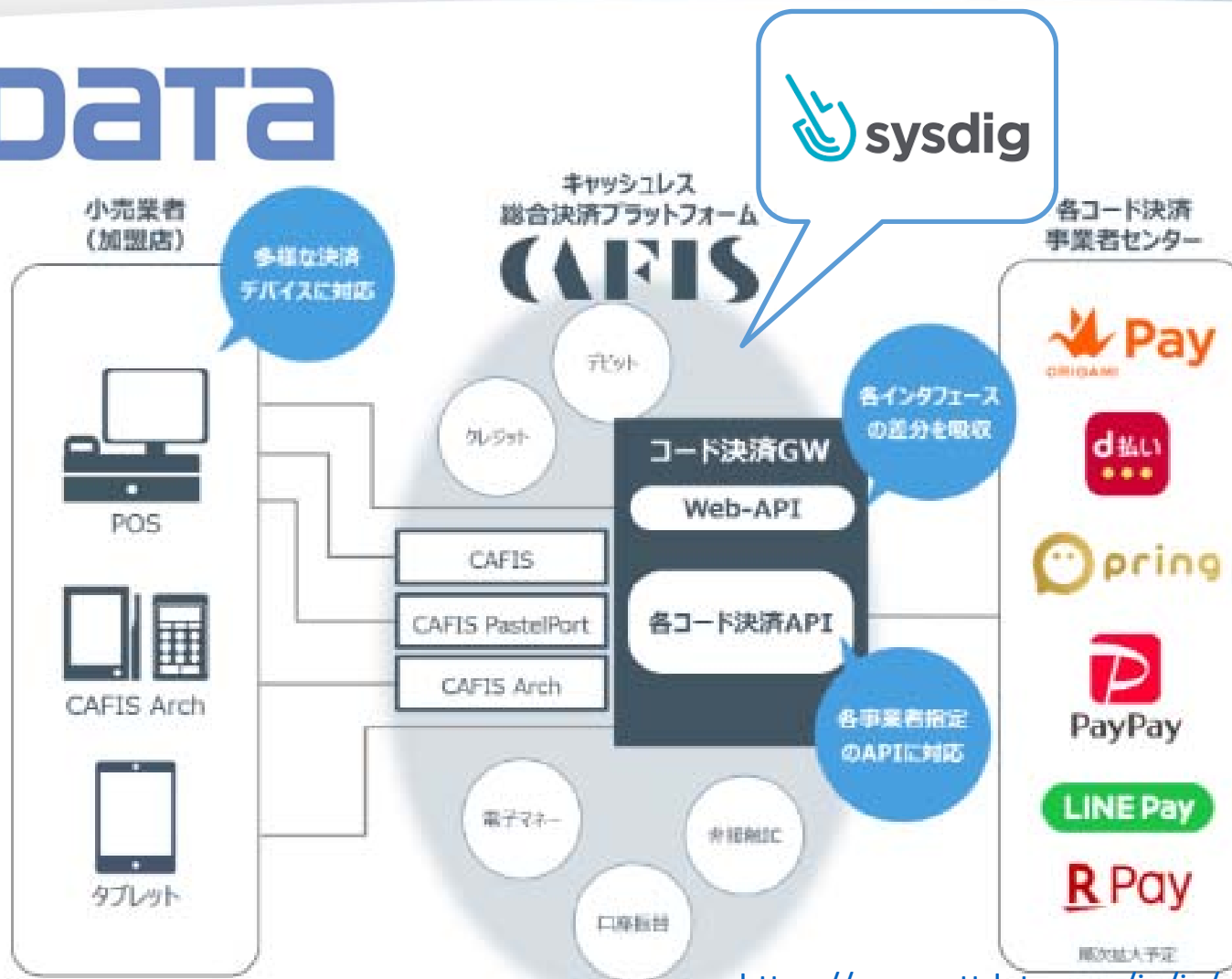


BNY MELLON



# 国内採用実績

## NTT Data



<https://www.nttdata.com/jp/ja/news/release/2018/121000/>

## SCSKとNTTデータ、コンテナセキュリティ領域におけるビジネスに関する業務推進を開始

～NTTデータが「Kubernetes」環境向けセキュリティ・モニタリングプラットフォーム「Sysdig Secure DevOps Platform」の販売パートナーに参画～

2020年7月16日

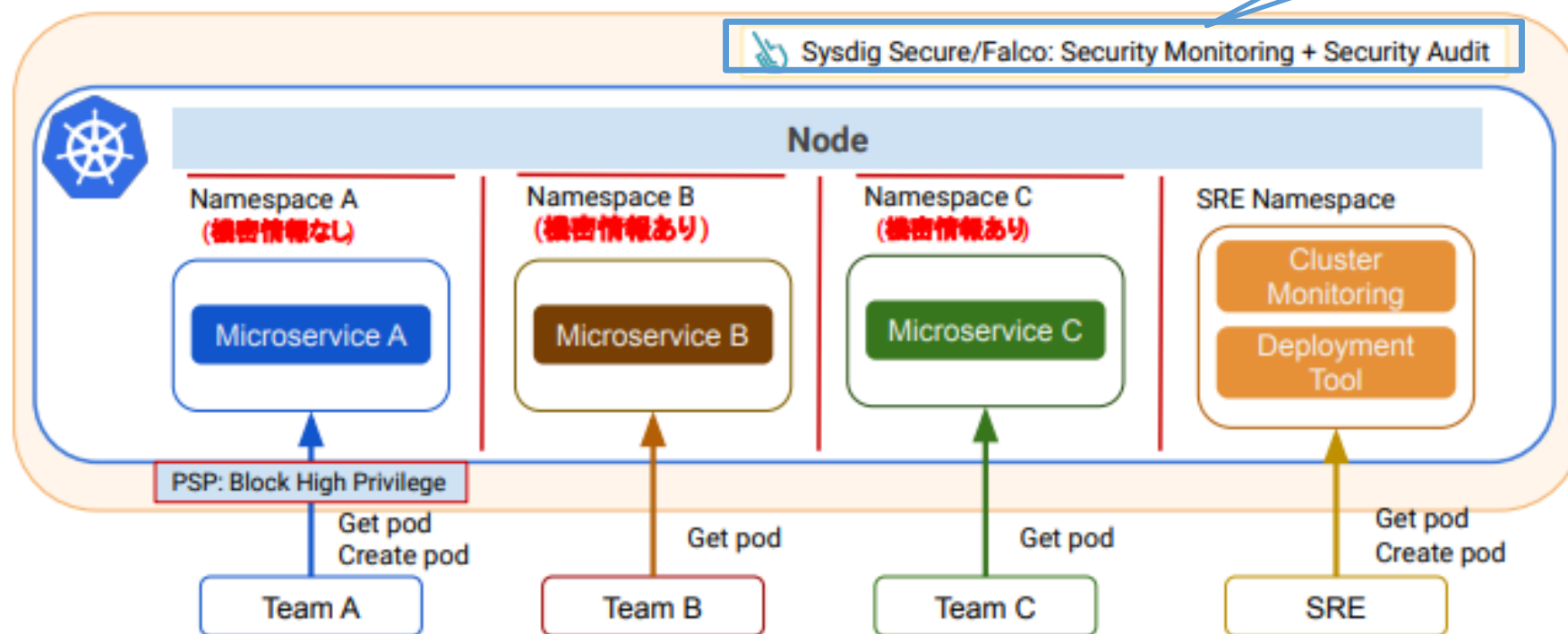
SCSK株式会社と株式会社NTTデータは、コンテナ管理オープンソースソフトウェア「Kubernetes(クーベネティス)」環境向けセキュリティ・モニタリングプラットフォーム「Sysdig Secure DevOps Platform(シスディグ セキュア デブオプス プラットフォーム)」のビジネスに関する共同での業務推進を2020年6月から開始しました。

「Sysdig Secure DevOps Platform」の活用により、コンテナ化したアプリケーションのトラブル対応の迅速化、セキュリティの向上が可能となり、より堅牢なコンテナ「Kubernetes」環境の実現が期待できます。

本提携により、NTTデータはSCSKの「Sysdig Secure DevOps Platform」販売パートナーに参画し「Sysdig Secure DevOps Platform」の販売を拡大して、2023年までに50億円の売り上げを目指します。

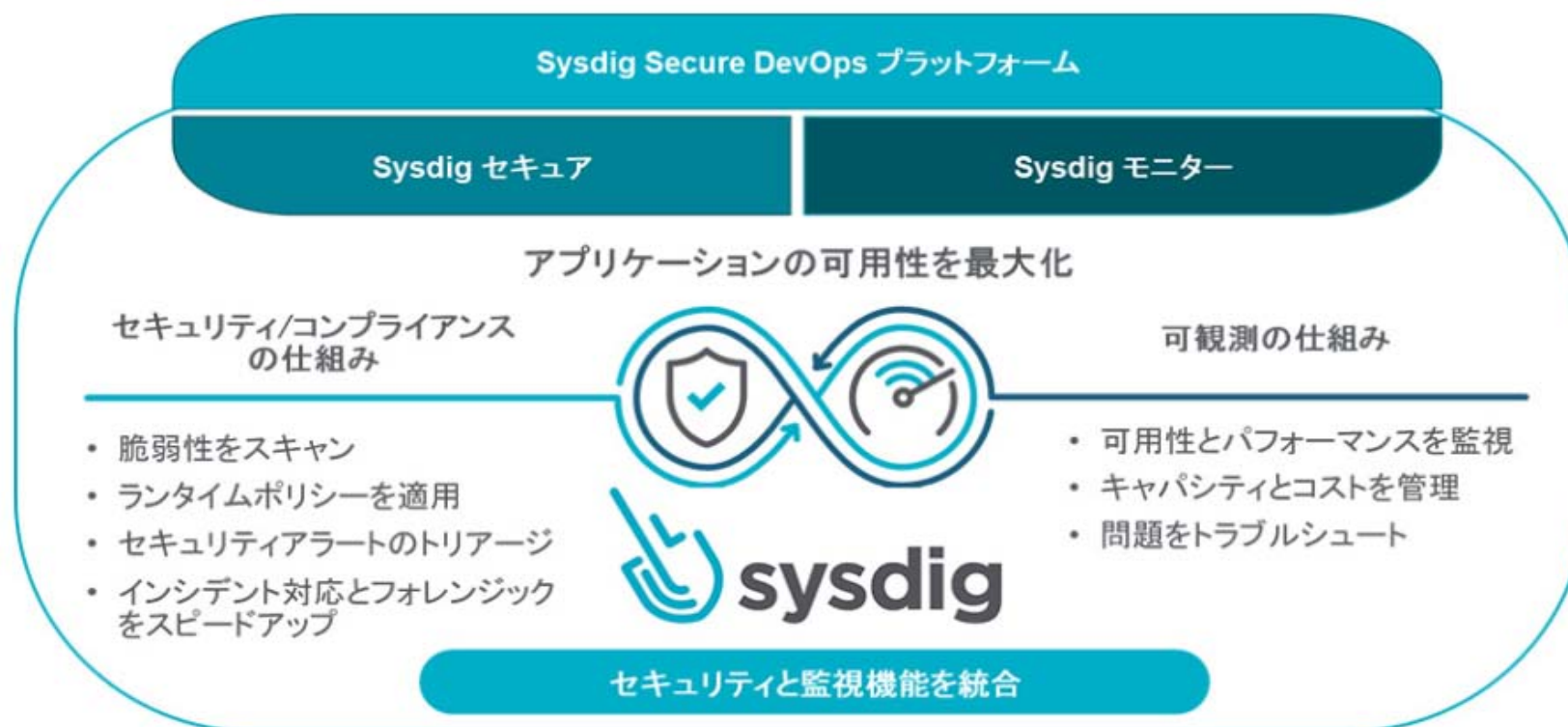
<https://www.nttdata.com/jp/ja/news/release/2020/071600/>

# 国内採用実績



# まとめ

- ☑ 管理するコンテナ数が増大 ➡ 課題は「監視とセキュリティ」
- ☑ Sysdigはコンテナ環境に特化し、監視・セキュリティ・トラブルシューティング・フォレンジックを一気通貫で提供できる唯一のソリューション



お問合せ先



Sysdig紹介サイト：

<https://www.scsk.jp/sp/sysdig/>

☆ブログ更新中！！

クラウドネイティブな環境を考慮した  
セキュリティの仕組みとは？

[https://www.scsk.jp/sp/sysdig/blog/kubernetes/post\\_1.html](https://www.scsk.jp/sp/sysdig/blog/kubernetes/post_1.html)

お問い合わせ先：

ITエンジニアリング事業本部  
ミドルウェア第二部



姜 来誠(きょう らいせい)

東京都江東区豊洲3-2-20 豊洲フロント  
電話：03-5166-1320  
Eメール：Sysdig-sales@ml.scsk.jp

