

The SCSK logo is rendered in a bold, blue, sans-serif font. The letters are thick and closely spaced, with a slight shadow effect on the right side of the letters, giving it a three-dimensional appearance. The background of the slide features several overlapping, thin blue circular lines that create a sense of motion and depth.

夢ある未来を、共に創る。

# HPC環境でのログ管理

splunk > ご紹介

---

SCSK株式会社  
プラットフォームソリューション事業部門  
ITエンジニアリング事業本部  
エンタープライズ第一部

2015年2月20日

1. ログ分析について
2. Splunkについて
3. 利用事例のご紹介

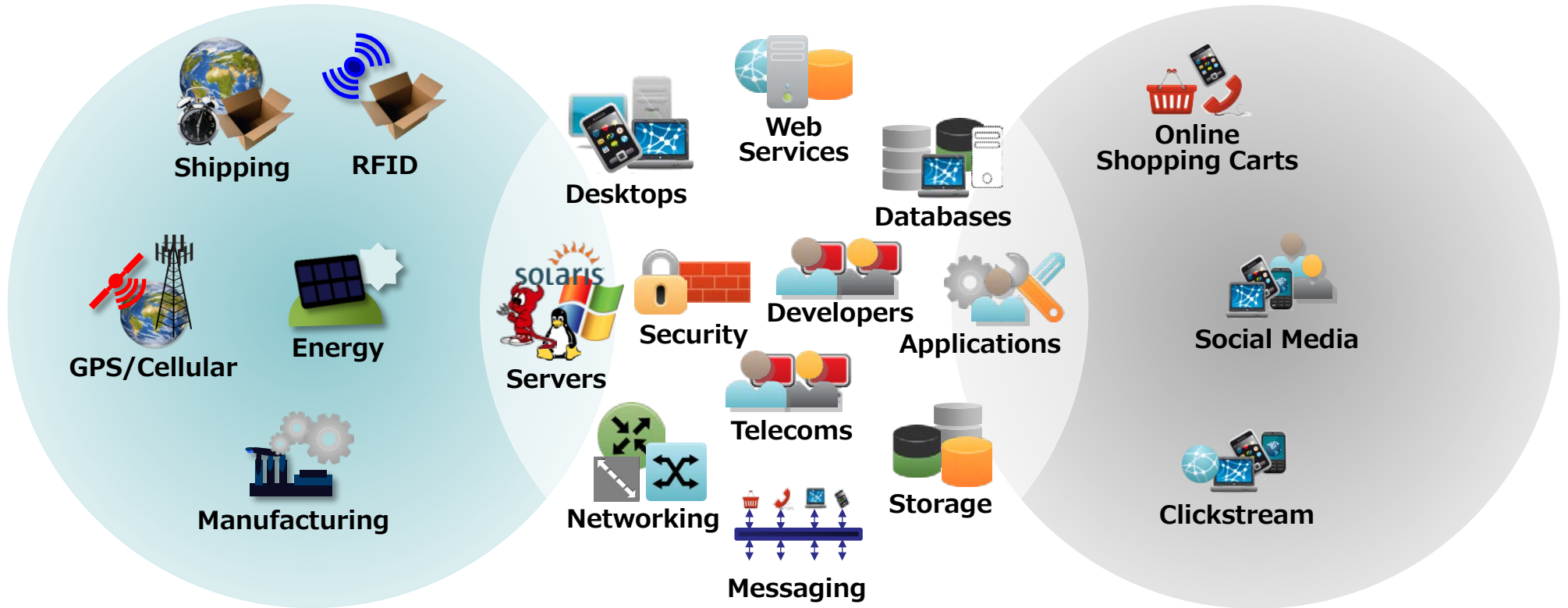
# 1. ログ分析について

企業内で起きていること =  
多くの企業内データはマシンから生成されます

様々なデータソース

コアIT環境ログ

お客様が目にするIT



クラウド



仮想環境



物理環境

# 1. ログ分析について

## ITシステムに問題が発生した時、 様々なマシンログが出力されています。



注文処理  
サーバ

ORDER,2012-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100



ミドルウェア  
エラー

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.  
Exception follows: weblogic.jdbc.extensions.ConnectionDeadSQLException:  
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The  
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:  
ACMEDB-01:1521. Reason: Connection refused



自動応答  
システム

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type  
0:19:9, App 0, ANI T7998#1, DNIS 5555685981, SerID 40489a07-7f6e-4251-801a-  
13ae51a6d092, Trunk T451.16  
05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092  
CUSTID 10098213  
05/21 16:37:49.732 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092



ツイッター

```
{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:  
"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},  
objectType:"person",preferredUsername:"B0ysF@n80",statusesCount:6072},body:"Just bought  
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if  
you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}
```

# 1. ログ分析について

Splunkに蓄積していれば、  
多様なログを結びつけ横串で分析することができます。



注文処理  
サーバ



ミドルウェア  
エラー



自動応答  
システム



ツイッター

カスタマーID

注文 ID

ORDER,2012-05-21T14:04:12.484,10098213,569281734,67.17.10.12,43CD1A7B8322,SA-2100

May 21 14:04:12.996 wl-01.acme.com Order 569281734 failed for customer 10098213.

Exception follows: weblogic.jdbc.extensions.CannotGetConnectionException:  
weblogic.common.resourcepool.ResourceDeadException: Could not create pool connection. The  
DBMS driver exception was: [BEA][Oracle JDBC Driver]Error establishing socket to host and port:  
ACMEDB-01:1521. Reason: Connection refused

注文 ID

カスタマーID

05/21 16:33:11.238 [CONNEVENT] Ext 1207130 (0192033): Event 20111, CTI Num:ServID:Type  
0:19:9, App 0, ANI T7998#1, DNIS 5555683981, SerID 40489a07-7f6e-4251-801a-  
13ae51a6d092, Trunk T451.16

05/21 16:33:11.242 [SCREENPOPEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

CUSTID 10098213

カスタマーID

05/21 [DISCEVENT] SerID 40489a07-7f6e-4251-801a-13ae51a6d092

ツイッター ID

{actor:{displayName:"Go Boys!!",followersCount:1366,friendsCount:789,link:  
"http://dallascowboys.com/",location:{displayName:"Dallas, TX",objectType:"place"},  
objectType:"person",preferredUsername:"GoBoys",statusesCount:6072},body:"Just bought  
this POS device from @ACME. Doesn't work! Called, gave up on waiting for them to answer! RT if  
you hate @ACME!!",objectType:"activity",postedTime:"2012-05-21T16:39:40.647-0600"}

# 2. Splunkについて

# Splunk® >

## Splunk Inc. 会社概要

2004年設立

本社：米国サンフランシスコ

支社：ロンドン、香港

社員数：1,300人

売上高：\$302.6M

(前年度比52%増)

## 7,900以上の顧客

世界100カ国で利用実績

フォーチュン100社中70社導

入済み

日本国内、約200社に導入済

み

最大取り込みログ量 300TB/

日

## 2. Splunkについて

### Splunk Inc. これまでの受賞歴

FAST COMPANY

#1 Big Data  
Innovator

#4 Most  
Innovative

Gartner

2013 SIEM Magic  
Quadrant LEADER

2012 IT Operations  
Market Growth

SCS MAGAZINE SCS MAGAZINE

AWARDS

2014

WINNER

Honored in the U.S.

AWARDS

2013

EUROPE

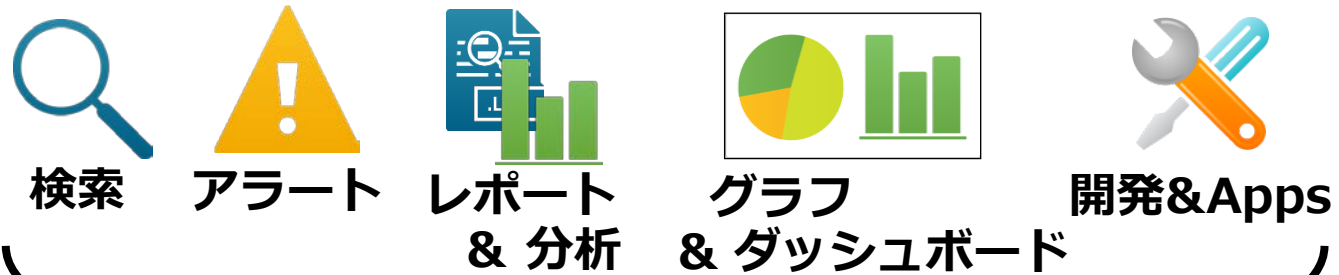
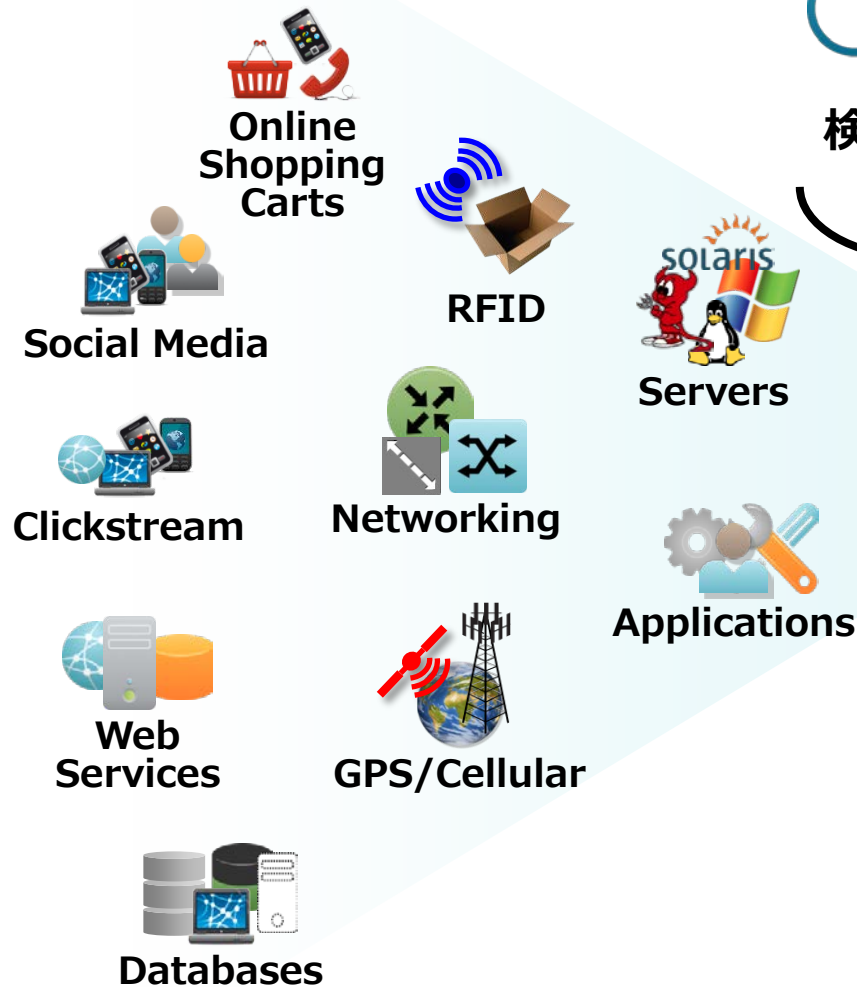
WINNER

Best Enterprise  
Security Solution

# 2. Splunkについて

あらゆるテキストログを収集/蓄積して、  
検索、分析、可視化するプラットフォームを提供します。

## 多様なデータソース

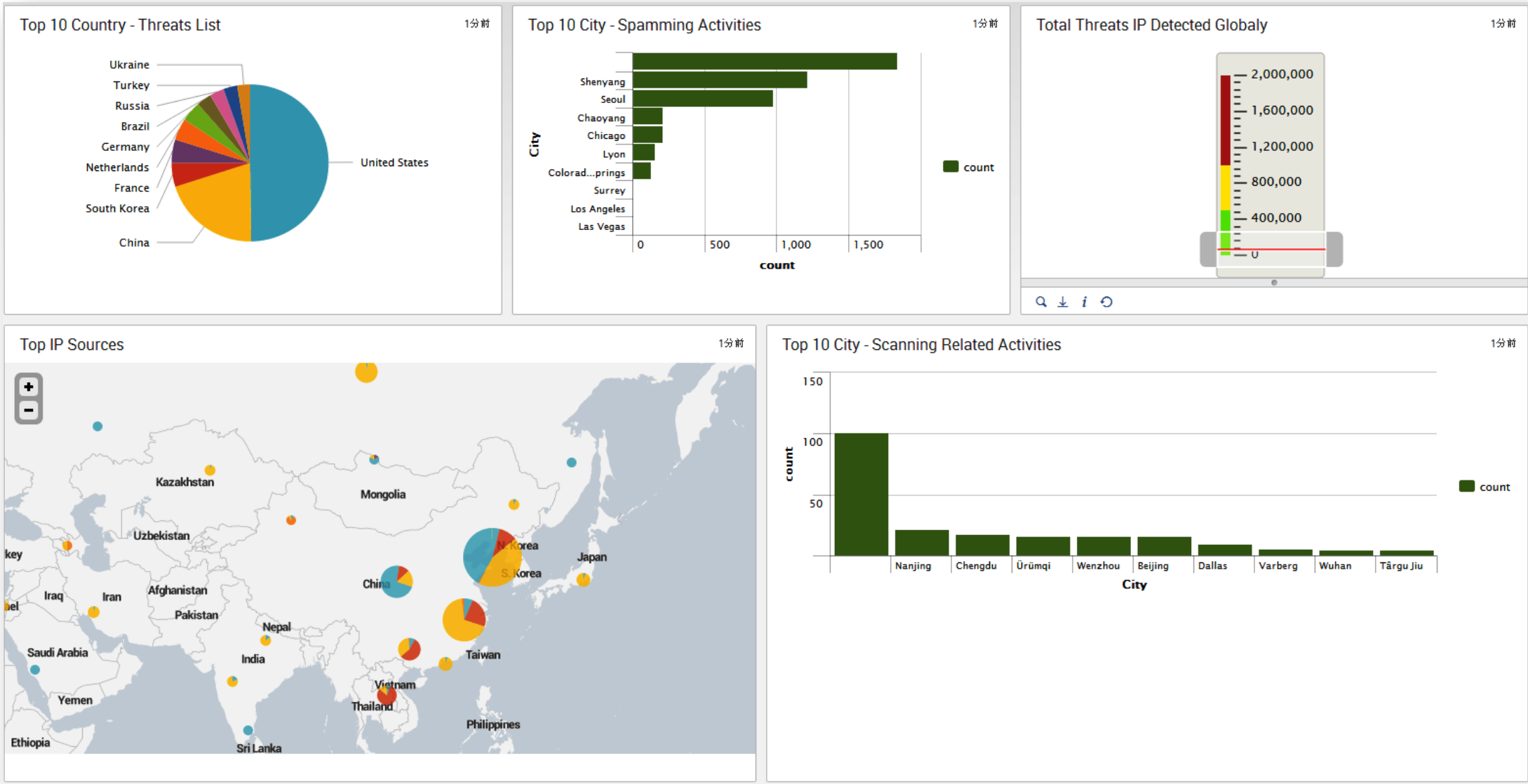


時間ベースの独自のデータベース  
“時間”を切り口に、高速な検索が可能



# 2. Splunkについて

グラフ、レポートを組み合わせて、  
ユーザ毎のダッシュボード画面として提供できます。



# 3. 利用事例のご紹介

2014年10月7日から9日にかけて行われたSplunk .conf2014にて講演された内容となります。

## Splunk利用団体

✓ Los Alamos National Laboratory

## HPC環境規模

✓ ラック数： 96ラック

✓ ノード数： ～9,000ノード

✓ CPUコア数： ～100,000core



## Splunkを利用したオペレーション

① HPC環境のベンチマーク・テスト結果を分析。

利用ログ：

各ベンチマーク結果ログ

(Memory Bandwidth Tests, IO Bandwidth Tests, CPU Speed Tests)

効果：

テスト結果を、簡単に視覚的に判断可能に

② HPC環境のシステム・モニタリング。

利用ログ：

Syslog, 各種リソース(CPU, Memory, Disk I/O, Netwok)利用値

効果：

サーバの利用状況を把握し易く

# Splunk トライアル版のご案内

The screenshot shows the SCSK website's navigation menu with categories like '製品・サービス' (Products/Services), 'イベント・セミナー' (Events/Seminars), 'ニュースリリース' (News Release), '株主・投資家情報' (Investor Relations), '採用情報' (Employment Information), and '企業情報' (Company Information). The main content area features a Splunk banner with the text 'splunk> Guide to Operational Intelligence' and 'あらゆるマシンデータを、価値ある情報に。' Below this are tabs for 'Splunkとは?' (What is Splunk?), 'ソリューション' (Solutions), '導入事例' (Case Studies), 'FAQ', and 'サポート' (Support). A sidebar on the left lists various Splunk-related links. A red circle highlights a green button at the bottom of the page that says 'フリー版 Splunk ダウンロード >' (Free Splunk Download >).

## Splunk トライアル版 (500MB/1日, 60日) へのリンク

|       |   |
|-------|---|
| 対応 OS | Linux2.6+ カーネルのLinux<br>ディストリビューション(x86並びにx86_64)                     |
|       | Solaris 10 & 11、Sparc   |
|       | Mac OS X 10.7, 10.8   |
|       | FreeBSD 6.1 以上(64bitは6.2以降)   |
|       | AIX 6.1, 7.1  |
|       | 32ビット Windows Vista、Windows 7/8、<br>Windows Server 2003/2008 R2       |
|       | 64ビット Windows Vista、Windows 7/8、<br>Windows Server 2003/2008 /2012 R2 |

<http://www.scsk.jp/product/common/splunk/>

グローバルITサービスカンパニーが、  
ついに始動。

システム開発から、ITインフラ構築、  
ITマネジメント、BPO、  
ITハード・ソフト販売まで、  
ビジネスに必要なすべてのITを、  
SCSKがフルラインナップでご提供します。



プラットフォームソリューション事業部門

ITエンジニアリング事業本部

ミドルウェア部

担当： 根本、川田、小山、西岡

Email : [splunk-sales@ml.scsk.jp](mailto:splunk-sales@ml.scsk.jp)

電話： 03-5166-1673

製品紹介URL : [www.scsk.jp/product/common/splunk/](http://www.scsk.jp/product/common/splunk/)

## 経営理念

私たちの使命

# 夢ある未来を、共に創る

お客様からの信頼を基に、共に新たな価値を創造し、  
夢ある未来を拓きます。

私たちの3つの約束

### 人を大切にします。

一人ひとりの個性や価値観を尊重し、互いの力を最大限に活かします。

### 確かな技術に基づく、最高のサービスを提供します。

確かな技術とあふれる情熱で、お客様の喜びと感動につながるサービスを提供します。

### 世界と未来を見つめ、成長し続けます。

全てのステークホルダーの皆様とともに、世界へ、そして未来へ向けて成長し続けます。

## 行動指針

### Challenge

未来を変える情熱を持ち、  
常に高い目標を掲げ、挑戦する。

### Commitment

お客様に対し、社会に対し、  
責任感を持ち、誠実に行動する。

### Communication

仲間を尊重し、心を通わせ、  
チームワークを発揮する。