

# iSHARE 2017年 初夏号

- ・連載『経営に役立つデータ分析：その差に意味があるだろうか？』
- ・IT ツール情報：Kaspersky Endpoint Security for Business

## 猛威をふるうランサムウェア..

2017年5月12日「ランサム(身代金)ウェア」による大規模なサイバー攻撃が発生し、テレビのニュースにも取り上げられるくらい大きな話題となりました。その名も「WannaCry(泣きたくなる)」と命名された悪意のあるソフトウェアが世界中に脅威を与えました。マイクロソフトは、既にサポートを停止した WindowsXP に対しても異例とも言える対策を取りました。如何にその影響が深刻だったかを物語っています。情報処理推進機構(IPA)が発表した「情報セキュリティ10大脅威 2017」では、企業

の脅威としてランサムウェアを2位に挙げています。ランサムウェアはアンチウイルスソフトでは防ぎきれません。感染することを想定した対策が重要です。セキュリティ対策は、

「如何に感染しないか」という対策では不十分で、「感染した後にどう復元させるか」という視点での対策が必要になってきています。弊社のIT110サポートでは、アンチウイルスソフトをランサムウェア感知に強いものに変更することと併せて、感染した場合の対策としてバックアップの強化を進めています。

順位	組織	昨年順位
1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	7位

(出典:情報処理推進機構、情報セキュリティ10大脅威 2017)

## ITフェア大阪 に参加しました..

弊社サービスがIT補助金の対象に認定されたことで、4月26日に大阪で開かれた「IT導入で商売繁盛！プラスITフェア」に参加する機会を得ました。「テレワークを実現するITインフラとは」をテーマに出展をしました。そこで気がついたことがいくつかありました。ひとつがテレワークへの関心です。「テレワークへの取り組みを会社から指示されて検討を始めた」という人事・総務の担当者が多いこと、テレワークをどう実現したらいいか具体的なイメージを持っている人が少なかったことは意外でした。また、その実現手段としてのシンクライアントを知る人が少なかったことは残念でした。働き方改革は、中小企業にとっても重要な経営課題となることは間違いのないと思います。その手段としてのテレワークを弊社の今後のテーマとして力を入れて行きたいと思っています。また、補助金への関心の高さも驚きでした。終日、IT補助金の説明会が開催されていましたが、満席状態でした。IT導入の障壁がコストにあることの現れでしょうか、補助金や助成金がIT導入のきっかけになることは間違いのないようです。

今年度は中小企業経営強化税制やテレワーク助成金などIT投資を後押ししてくれる支援策が充実しています。IT投資には絶好の機会です。ランサムウェア対策やテレワークの取り組みなど前向きに対策を進めることをお奨めします。



iSHARE 早春号に掲載した「経営に役立つデータ分析」はとても好評で、「統計を身近なテーマでわかりやすく解説してあり良かった！」など、メールも含め、多くの方から好評いただきました。

前回に引き続き、事例とともに**統計的仮説検定**をテーマにお届けします。

- ここは名古屋商事の社長室です。最近の経営課題は営業力の強化です。そのため数ヵ月前に外部コンサルタントを呼んで、2泊3日の営業力強化合宿研修を実施しました。今日は熱田営業部長からその合宿研修の成果についての報告を受けています。



熱田営業部長

研修後のアンケートでは参加者の評判は良く、良い以上が全体の80%を占めています。  
 今日はその研修効果を判断すべく営業部員20名の研修前と研修後の営業実績表を持参しました(図表1)。  
 ご覧のように研修前の平均売上高は849.7万円でしたが、研修後は892.2万円と、研修前よりも5%上回っています。  
 これは行った研修による効果だと思われるので、今後も適宜この研修を実施したいと考えています。

【図表1】基礎データ  
営業員実績表(単位:百万円)

営業員	研修前	研修後
A	905	958
B	1059	1160
C	742	995
D	956	901
E	737	745
F	996	901
G	915	1076
H	862	1037
I	1033	1035
J	1008	1069
K	750	806
L	630	861
M	635	623
N	896	666
O	764	625
P	1065	1147
Q	580	563
R	689	862
S	753	752
T	1017	1062
平均	849.7	892.2
伸び率		5.0%

確かに平均売上は849.7万円から892.2万円と42万円、5%伸びているが、この差は偶然ではないのか。差に意味(有意差)はあるのだろうか？



名古屋社長

- 社長の発言を聞いた営業部データ分析スタッフは、早速分析を行い、その結果を社長に報告しました



分析スタッフ

差に意味があるのかどうかの検定(統計的有意差検定)を行ってみました。  
 分析シートをご覧ください。図表2と3はともにExcelによる分析ですが、2はオートマチックタイプ、3はマニュアルタイプの違いだけで結果は同じです。  
 いずれもP値が0.06と0.05よりも大きいですので帰無仮説を棄却できず、有意とは認められませんでした。すなわちこの差は偶然と考えられますので、研修に効果があるとは言えません。営業力強化という課題については営業部員との意見交換やアンケート調査、ヒヤリング調査など広く情報収集された上で決定されることをお勧めいたします。



【分析シート】

有意差検定:有意水準0.05  
 帰無仮説:研修前の売上と研修後の売上に差はない  
 対立仮説:研修前の売上と研修後の売上に差はある

【図表2】Excelの分析ツールを使用

t-検定: 一対の標本による平均の検定		
	00年	01年
平均	849.6689	892.1523
分散	24346.34	33771.85
観測数	20	20
ピアソン相関	0.755395	
自由度	19	
t	-1.56187	
P(T<=t) 片側	0.067411	
t境界値 片側	1.729133	
P(T<=t) 両側	0.134821	
t境界値 両側	2.093024	

【図表3】Excel関数を使っての手動計算

項目	研修前	研修後	前後差	備考
平均値	849.7	892.2	42	A~Tの平均
分散	24346.336	33771.855	14797.204	=VAR.S(データ範囲)
サンプルサイズ			20	=A~Tの行数
自由度			19	=サンプルサイズ-1
差の標準誤差			27.200371	=(分散/サンプルサイズ)^0.5
t値			1.56187	=差の平均値/差の標準誤差
p値			0.0674105	=T.DIST.RT(t値,自由度)
t値境界値			1.72913	=ABS(T.INV(0.05,自由度))

(注) ExcelのTTEST関数を使う方法もありますが同じ答えですので割愛しています

なるほど、ご苦労様、ありがとう。

調査して何が問題なのかを明確にする必要があるな。

関係者を交えて今後の事を話し合ってみよう！



名古屋社長

【今回の視点】

今回は**統計的仮説検定**の事例です。**統計的仮説検定**には目的に応じて様々な種類がありますが、ここでは営業研修のビフォー/アフターにおける売上差に意味があるかどうかを探る平均の差の検定(『t-検定』と呼ばれるもの)です。事例では2群ですが、3群以上の場合は分散分析、多重比較といった手法を使います。**統計的仮説検定**は様々な場面で意思決定に活用することができます。

さて、**統計的仮説検定**では有意となれば、「それは偶然に起きたことではない=要因によって結果が左右された」と判断します。ビジネスでは差に着目することが多くありますが、その差が有意かどうかを問うことはあまりみかけません。有意かどうかを探るには2つのケースがあります。

一つはこの事例のように要因が分かっているその要因の影響度を探る場合、もう一つは“有意差有り”との判定から逆にその差をもたらしている要因は何かを探る場合です。意思決定プロセスにこのような手法を加えることでビジネスの背景にある規則性に迫ることができるのではないのでしょうか。ただ、経営者がこれらの分析手法をマスターする必要はありません。担当者一言「差に意味はありますか?」、あるいは「その差は有意ですか?」と質問すればいいかと思います。



藤井統計実務研究所  
 代表 藤井 博

【プロフィール】山口県岩国市出身。大学卒業後当時ベンチャー企業であった通販会社に入社。取締役、常務取締役、関係会社の社長、会長を経て、2013年9月、統計的(科学的)手法による意思決定・問題解決を主業とする藤井統計実務研究所を開設。主業の対象領域としては問題解決、物流改善、事業分析、人事科学等がある。

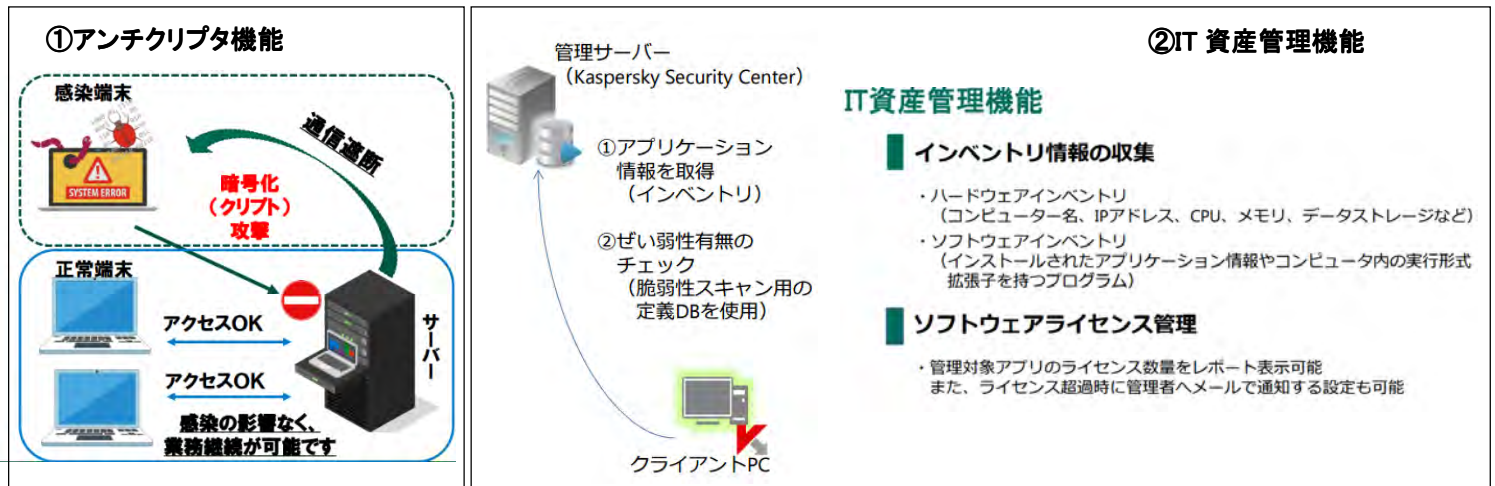
データ解析士、物流技術管理士の資格を有す。京都商工会議所会員、日本物流資格士会員。

ホームページ: <http://fujii-metrics.com>



サイバー攻撃(ランサムウェアなどの迷惑メール)の増加に伴い、弊社ではセキュリティ強化提案をしていますが、その1つ、『Kaspersky Endpoint Security』をご紹介します。

Endpoint(エンドポイント)というのは、ネットワークの一番最終の端末(パソコンやタブレットなど)を指します。Kaspersky(カスペルスキー)社製品の大きな特長を2つ解説します。



### ①ファイルサーバー向けランサムウェア対策機能(アンチクリプタ)を搭載

ランサムウェアの暗号化通信を検知すると、対象コンピュータからの接続を遮断する機能です。ウイルス自体を検知するのではないため、比較的高確率にランサムウェア被害を抑えられます。

### ②アンチウイルスソフトウェア機能に加えて「IT 資産管理機能」を搭載

近年のサイバー攻撃は OS やアプリケーションの脆弱性を狙います。Windows Update や アプリケーションの更新をしていないとアンチウイルスが正常に稼働していても感染するリスクが高まります。パソコンやサーバーのアップデートの管理がセキュリティ強化の重要なポイントになります。ただ、1台1台確認するのは大変で漏れが出る可能性があります。その管理に利用するのが、『IT 資産管理ツール』です。『IT 資産管理ツール』を利用すれば、「自社内にコンピュータが何台あるのか?」「どんなアプリがインストールされているのか?」、更には、「USB メモリ利用を禁止する」などの管理が可能です。他社メーカー製で有名な「SkySea(スカイシー)」がありますが、導入コストがかなり高くなります。Kaspersky の Endpoint Security for Business はアンチウイルス機能に加え、IT 資産管理機能も備えていて、強固な対策をすることが可能です。

通常のアンチウイルスソフトウェアよりも金額は少し上がりますが、ランサムウェア対策と資産管理を同時に実現するツールとしてご検討をお奨めします。

INFINITY

2017年06月発行  
発行：株式会社インフィニティ

〒460-0002  
愛知県名古屋市中区丸の内3-17-29 丸の内iaビル 7F  
TEL : 052-228-0417 FAX : 052-228-0428  
URL : <http://www.infinity-i.co.jp>  
メールアドレス : [support@infinity-i.co.jp](mailto:support@infinity-i.co.jp)