# 2016 年 情報漏えい時に発生するコストに関する 調査:
## 事業継続マネジメント (BCM) の効果

IBM の依頼によるベンチマーク調査
実施: Ponemon Institute 社
2016 年 6 月

# 2016 年[1] 情報漏えい時に発生するコストに関する調査:
## 事業継続マネジメント (BCM) の効果

Ponemon Institute、2016 年 6 月

### 第 1 部: はじめに

2016 年 IBM が依頼した「*2016 年 情報漏えい時に発生するコストに関する調査: 事業継続マネジメント (BCM) の効果*」は、情報漏えいの発生に先立って BCM プログラムを実施することの財務と評判に関するメリットを分析しています。本調査によると、BCM プログラムにより、情報漏えいの 1 件当たりのコストを削減して、情報漏えいの検出と被害拡大防止にかかる平均時間を短縮し、今後 2 年間におけるインシデントの発生確率を減少させることができます。[2]

BCM に関する本調査は、情報漏えいの経済的影響を定量化して長期的なコストの傾向を観察している「*2016 年 情報漏えいのコストの調査: グローバル調査*」の一環として実施されています。本年のグローバル
調査では、情報漏えいの 1 件当たりの平均コストは 154 ドルから 158 ドルに増加しました。情報漏えいの総コストは 380 万ドルから 400 万ドルに増加しました。[3]

本年の調査には、米国、英国、ドイツ、オーストラリア、フランス、ブラジル、日本、イタリア、インド、アラブ地域、カナダ、そして初参加の南アフリカを代表する 16 業種の 383 社の企業が参加しました。参加企業はいずれも、被害レコード数が約 3,000 件から 101,500 件近くの情報漏えいを経験しています[4]。本調査では、被害レコードを、情報漏えいにおいて情報の紛失または盗難に遭った個人を特定するレコードと定義します。

グローバル調査の対象となった企業の大半 (52%) が、エンタープライズ・リスク管理、災害復旧、危機管理に BCM の職務やチームを関与させています。こうした専門家は、企業で情報漏えいが発生したときに関与しており、関与した結果として情報漏えいの問題解決の効率が向上し、発生コストが減少しています。

以下に、本年の調査対象の企業が BCM プログラムから得られたメリットのキー・ポイントをまとめます。

**情報漏えい時に発生するコストに対する事業継続マネジメント・プログラムの効果**

- 情報漏えいの 1 件当たりのコストが 9 ドル減少
- 情報漏えいの 1 件当たりのコストが 11% 減少
- 情報漏えいの総コストが 15% 減少
- 情報漏えいの検出にかかる平均時間が 52 日短縮
- 情報漏えいの被害拡大防止にかかる平均時間が 36 日短縮
- 今後 2 年間の情報漏えいの発生確率が 29% 減少

- **BCM の関与により、情報漏えいインシデントの検出にかかる平均時間と被害拡大防止にかかる平均時間が大幅に短くなる。**
具体的には、BCM を関与させていない企業では、情報漏えいの検出に平均 227 日間かかっています。対照的に、BCM を関与させている企業で情報漏えいの検出にかかった時間は平均 175 日でした。同様に、情報漏えいの被害拡大防止にかかった時間は、BCM を関与させていない企業では平均 88 日、BCM を関与させている企業では平均 52 日でした。

- **重大な情報漏えいの検出と被害拡大防止にかかる日数を合計でどれだけ短縮できるかは 16 業種で異なる。**教育と小売業の企業では、重大な情報漏えいの検出と被害拡大防止にかかる日数を、それぞれ 115 日と 109 日短縮できました。金融サービスは、68 日短縮できました。

---

[1]本レポートでは、作業完了日ではなく発行年を明記しています。本レポートで調査されている情報漏えいインシデントの大多数は、2015 年に発生したものです。
[2]インシデント対応プロセスを支える BCM チームには、災害復旧の職務に就いている担当者が含まれます。
[3]現地通貨は米ドルに換算しています。
[4]「被害レコード 1 件当たりのコスト」と「1 件当たりのコスト」は、本レポートでは同様の意味を持ちます。

- **情報漏えいインシデント対応の計画と実施への BCM の関与は非常に重要である。**本グローバル調査の対象となった 383 社の企業のうち 199 社の企業が情報漏えいによりもたらされる結果の解決に BCM を関与させていると自己報告しました。これらの企業の大半 (65%) が、その関与を非常に重要であると評価しています。

- **情報漏えいインシデント対応の計画と実施の一環として BCM を関与させていなければ、情報漏えい時に発生するコストはさらに高額になる。**紛失または盗難に遭ったレコード 1 件当たりの平均コストは 167 ドルになりえます。BCM を関与させていると、平均コストは 149 ドルと低くなります。同様に、BCM を関与させている場合と関与させていない場合の情報漏えいの総コストはそれぞれ、371 万ドルと
429 万ドルです。

- **BCM の関与による 1 日当たりのコスト節約は相当な額である。**情報漏えいインシデントの検出と被害拡大防止における効率により、1 日当たりのコストを節約できることが推定されます。図から分かるように、BCM を関与させている企業は、情報漏えいへの対応の被害拡大防止段階で 1 日当たり平均 6,591 ドルを節約しています。

- **インシデント対応計画の一環として BCM を関与させていない企業の方が、今後、情報漏えいが発生する可能性が高い。**本調査の結果では、情報漏えいに対する計画に BCM が関与していない場合には今後 2 年間に情報漏えいが発生する確率が 29% になることが明らかになりました。一方、BCM を関与させている場合は、この確率は 22% に下がります。

- **情報漏えいインシデント対応の計画と実施において自社の BCM チームを関与させている企業の割合はドイツと日本が最も高い。**BCM の関与が最も低い国はブラジルとアラブ地域です。イタリアを除き、すべての国で情報漏えいインシデント管理プロセスへの BCM の関与の度合いが高まっています。

- **BCM は、情報漏えいが発生した場合の事業運営の中断を最小限に抑える。**調査によると、BCM を関与させていない企業の 78% で重大な事業運営の中断が発生しました。BCM を関与させている企業では、この割合は 52% に減少します。

- **BCM の関与により、IT 運用のレジリエンスが改善される。**BCM を関与させていない企業の 75% が IT 運用に重大な中断が発生したと報告しています。対照的に、BCM を関与させている企業のうち、IT 運用に重大な中断が発生したと報告したのは 55% でした。

- **BCM は情報漏えい発生後の企業評価を保護できる。**本調査対象の企業の 55% が、情報漏えいが原因で企業評価やブランドに悪影響が生じたと報告しています。ただし、BCM を関与させていない企業では、(はるかに大きな割合の) 60% が企業のブランドと評価に影響が生じたと報告しました。

情報漏えいインシデント対応プロセスの管理担当者に対する 33 回の聞き取り調査に基づく詳細分析では、BCM プログラムが財務と評判に関する以下のメリットとして役立っている理由が明らかになりました。

- 厳格な計画とテストへの方向性を形成する
- 危機発生時にアップストリームとダウンストリームの通信チャネルが可能になる
- インシデント対応プロセスの複雑さを軽減する構造を確立する
- BCM のポリシー、計画、標準に準拠する結果として危機的なイベントに関する組織の判断力と認識を高める
- 重大なリスクの事前対応型の管理を支援するリーダーシップと専門知識を実現する
- 事前対応型の監視と警戒を受け入れる文化を発展させる

## 第 2 部: 主な調査結果

次の表に、本グローバル調査の対象とした 12 カ国、凡例、企業数、通貨をリストします。また、年次調査を行った年数が国ごとに、南アフリカの 1 年から米国の 11 年の範囲で示されています。

**表 1. グローバル調査の概要**

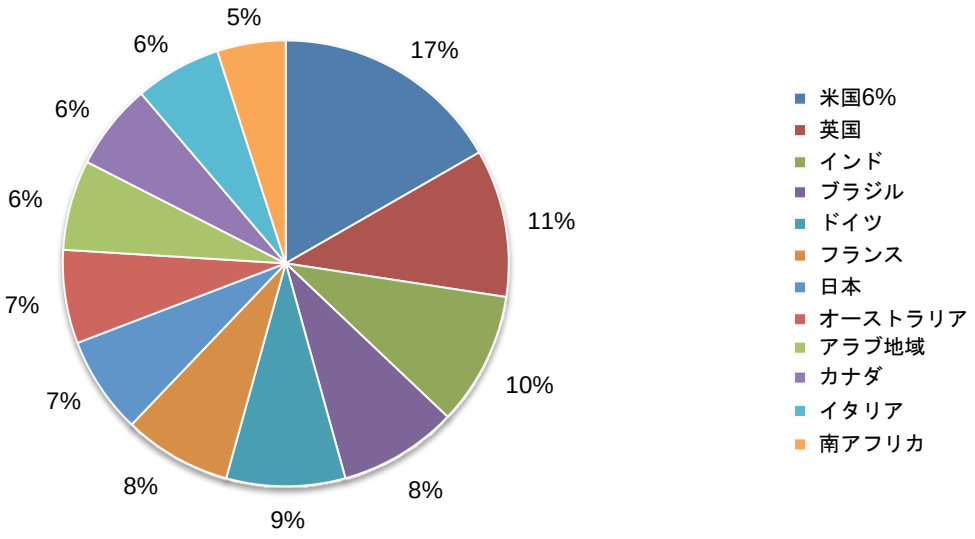
| 凡例 | 国名 | 企業数 | 割合 (%) | 通貨 | 調査対象年数 |
|---|---|---|---|---|---|
| AB | アラブ地域* | 25 | 7% | AED/SAR | 3 |
| AU | オーストラリア | 26 | 7% | AU ドル | 7 |
| BZ | ブラジル | 33 | 9% | レアル | 4 |
| CA | カナダ | 24 | 6% | CA ドル | 2 |
| DE | ドイツ | 33 | 9% | ユーロ | 8 |
| FR | フランス | 30 | 8% | ユーロ | 7 |
| ID | インド | 37 | 10% | ルピー | 5 |
| IT | イタリア | 24 | 6% | ユーロ | 5 |
| JP | 日本 | 27 | 7% | 円 | 5 |
| SA | 南アフリカ | 19 | 5% | ZAR | 1 |
| UK | 英国 | 41 | 11% | GBP | 9 |
| US | 米国 | 64 | 17% | US ドル | 11 |
| | | 383 | 100% | | |

*AB はサウジアラビアとアラブ首長国連邦の企業を混合したサンプルです。

次のグラフは、12 カ国内の参加企業 383 社の内訳を示したものです。図から分かるように、サンプル数が最も多いのは米国の 64 社、最も少ないのは南アフリカの 19 社です。

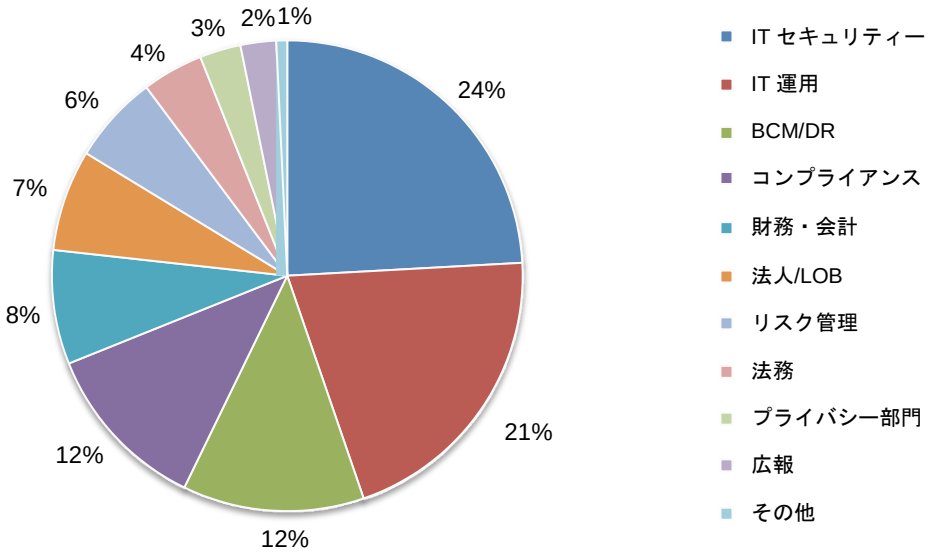
**円グラフ 1. 国別のベンチマーク・サンプルの割合**

対象: 全企業 (n=383)



円グラフ 2 は、12 カ国 383 企業を代表する、聞き取り調査に参加した 1,596 名の内訳を示しています。調査対象者の 24 パーセントが IT セキュリティー (例: SecOps)、21 パーセントが IT 運用に従事しています。

**円グラフ 2. 職務別の聞き取り調査回答者の割合**
対象: 全回答者 (n=1,596)



**情報漏えい時に発生するコストは、情報漏えいインシデントの検出と被害拡散防止にかかる平均時間と直接的に関連しています。**本年の調査では、情報漏えいの平均検出時間 (MTTI) と情報漏えいのコストには正の相関が認められることが判明しました。図 1 は、BCM を関与させている企業の方が、情報漏えいの検出にかかる時間が短いことを示しています。具体的には、2016 年には 52 日、2015 年には 56 日、時間が短縮されました。

**図 1. インシデント対応プロセスに BCM を関与させている企業と関与させていない企業の MTTI (Mean Time To Identify: 平均検出時間)**

MTTI の差 (2016 年 = 52 日、2015 年 = 56 日) MTTI の割合の差 (2016 年 = 26%、2015 年 = 27%) 対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社)

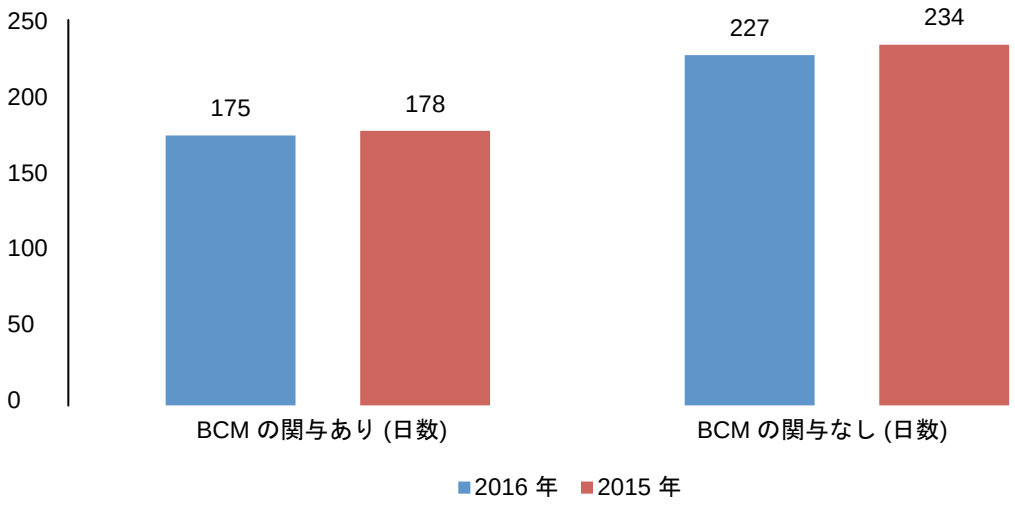
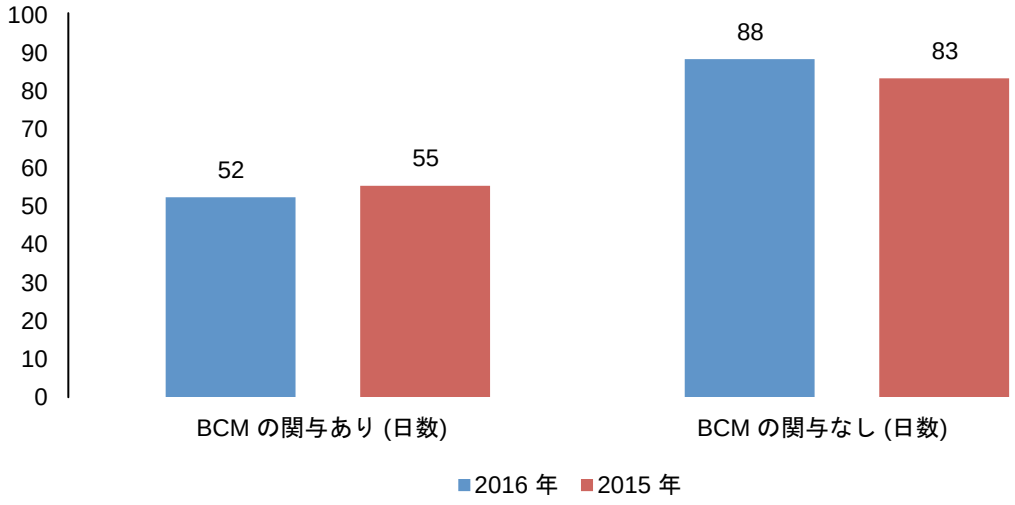



図 2 も同様の関係を示しています。つまり、BCM を関与させている企業では、情報漏えいインシデントの被害拡散防止にかかる日数がはるかに少なくなります。2016 年は 36 日、2015 年は 28 日、時間が短縮されました。

**図 2. インシデント対応プロセスに BCM を関与させている企業と関与させていない企業の MTTC (Mean Time To Contain: 平均被害拡散防止時間)**

MTTC の差 (2016 年 = 36 日、2015 年 = 28 日)
MTTC の割合の差 (2016 年 = 40%、2015 年 = 41%)
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社)



次のグラフは、本年の調査の参加企業 383 社の業種別の内訳を示したものです。円グラフ 3 は、16 業種の内訳を示しています。

**円グラフ 3. 業種別のベンチマーク・サンプルの割合**
対象: 全企業 (n=383)

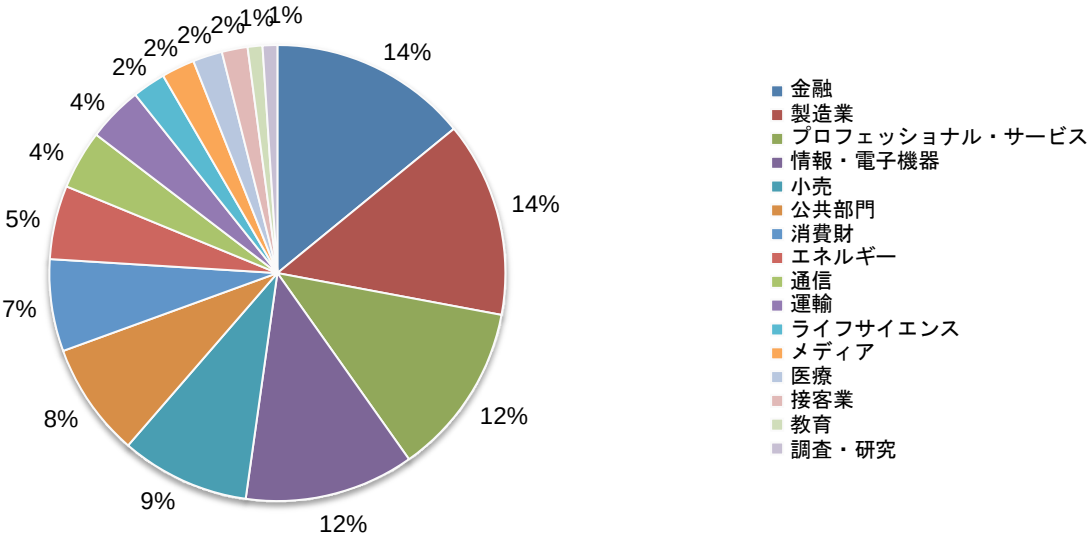



図 3 は、16 業種において重大な情報漏えいの検出と被害拡散防止で短縮できた合計日数を示しています。最も多くの日数を短縮できたのは、教育と小売業で、それぞれ 115 日と 109 日でした。最も少なかったのは金融サービスで、68 日でした。

**図 3. BCM の関与の結果として短縮できた MTTI と MTTC の合計日数**
短縮できた平均日数 (2016 年 = 88 日) 対象: 全企業
(n=199)

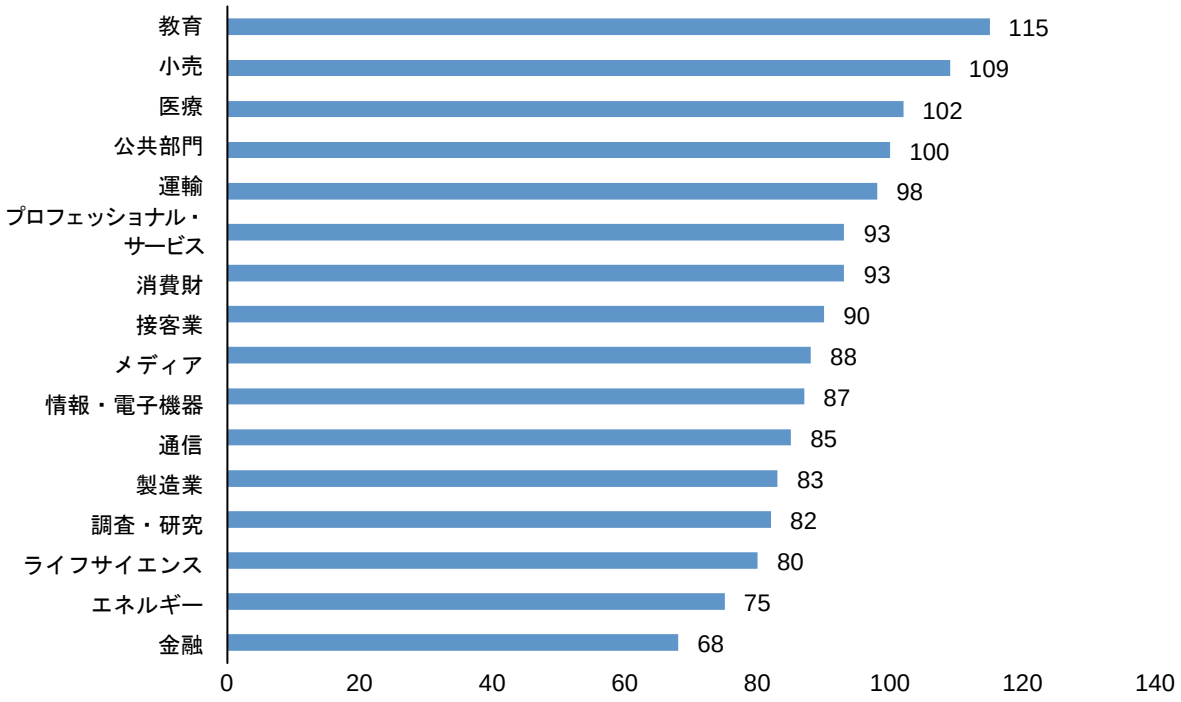


図 4 は、MTTI と MTTC の効率による 1 日当たりの推定コスト節約額を示しています。図から分かるように、BCM を関与させている企業は、88 日間で 1 日当たり平均 6,591 ドルを節約しています。昨年の推定節約額は 84 日間で 5,952 ドルでした。

**図 4. BCM の関与による 1 日当たりのコスト節約額**

BCM の関与による総コスト節約額 (百万米ドル単位) (2016 年 = $.580、2015 年 = $.500) 短縮できた MTTI と MTTC の合計日数 (2016 年 = 88 日、2015 年 = 84 日)
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社)

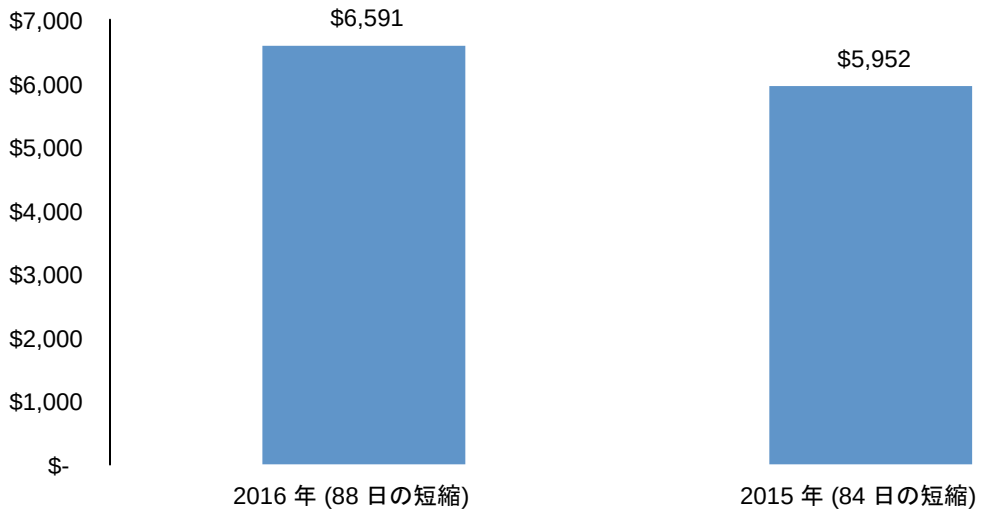



表 2 は、業種別の潜在的なコスト節約額を示しています。図から分かるように、最も多くのコストを節約できる可能性があるのは教育です。一方、最も低いのは金融サービスです。

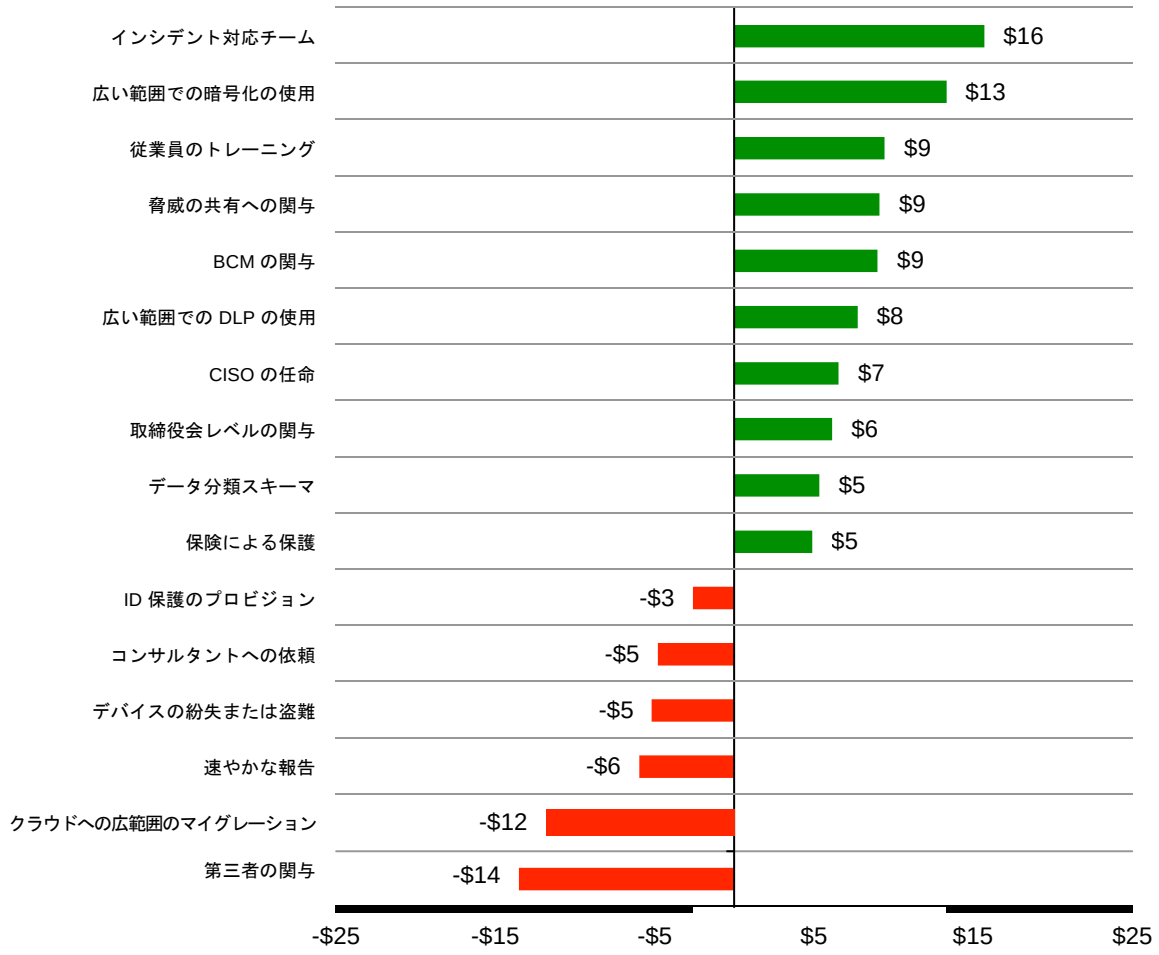
| 表 2: 業種別の推定コスト節約額 | 短縮日数 | 総コスト節約額* |
|---|---|---|
| 教育 | 115 | $757,965 |
| 小売 | 109 | $718,419 |
| 医療 | 102 | $672,282 |
| 公共部門 | 100 | $659,100 |
| 運輸 | 98 | $645,918 |
| 消費財 | 93 | $612,963 |
| プロフェッショナル・サービス | 93 | $612,963 |
| 接客業 | 90 | $593,190 |
| メディア | 88 | $580,008 |
| 情報・電子機器 | 87 | $573,417 |
| 通信 | 85 | $560,235 |
| 製造業 | 83 | $547,053 |
| 調査・研究 | 82 | $540,462 |
| ライフサイエンス | 80 | $527,280 |
| エネルギー | 75 | $494,325 |
| 金融 | 68 | $448,188 |

*2016 年のコスト節約額は、各業種の短縮日数に 6,591 ドルを乗算したものです。

**情報漏えい時に発生するコストに影響する要因。**この分析の文脈において、16 種類の各要因について正数 (緑で表示) はコストの削減分、負数 (赤で表示) はコストの増加分として定義されています。

図 4 に示すように、強力なインシデント対応チームが存在していると、情報漏えいの 1 件当たりのコストが最も大きく減少します。事業継続マネジメント (BCM) は、情報漏えいのコストを被害レコード 1 件当たり平均 9 ドル削減します。

**図 4. 情報漏えい 1 件当たりに発生するコストに対する 16 種類の影響要因**
対象: 全企業 (n=383)、単位: 米ドル



**インシデント対応計画に対する BCM の貢献。**図 5 に、情報漏えいのインシデント対応の計画と実施における BCM の関与をまとめています。本グローバル調査の対象となった 383 社の企業のうち 199 社、つまり 52% が BCM を関与させていました。残りの 184 社の企業は、BCM チームを関与させていなかったか、臨時でのみ BCM を関与させていました。昨年の分析では、50% の企業が情報漏えいのインシデント対応に BCM を関与させていました。

**図 5. 情報漏えいインシデント対応プロセスにおいて BCM はどのように役立っていますか?**
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)

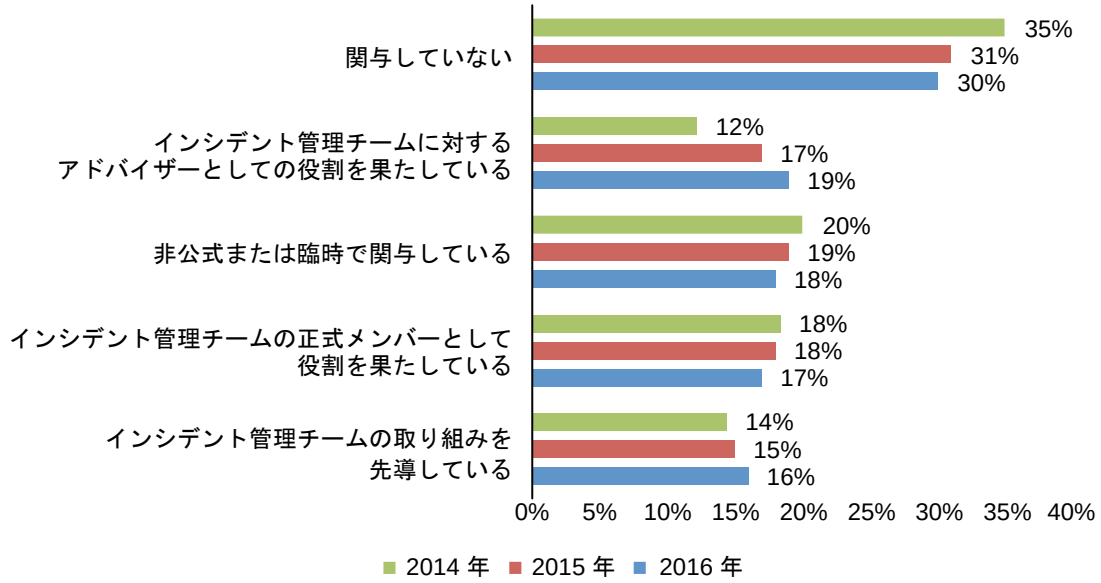
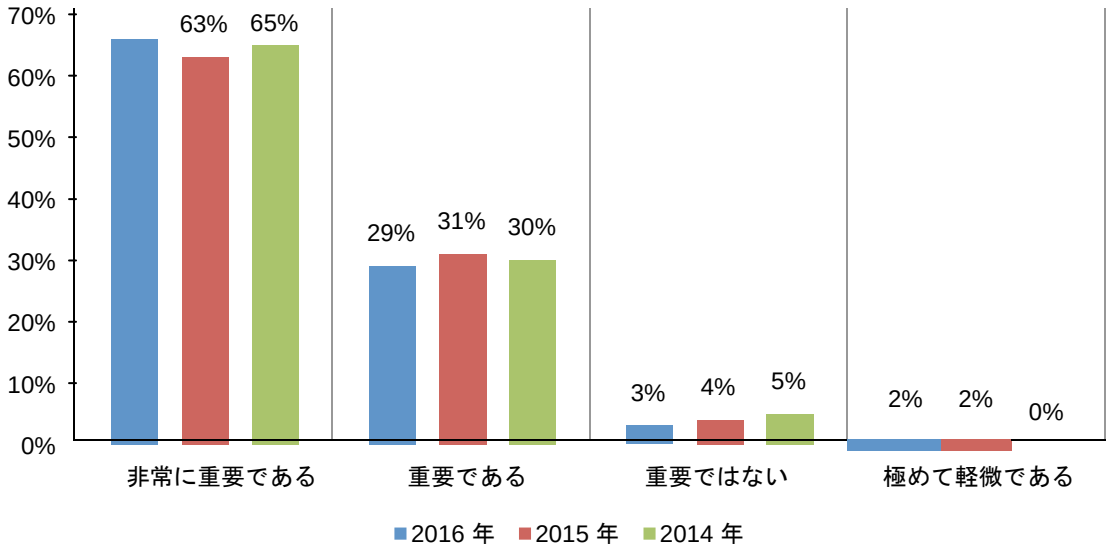



図 6 は、インシデント対応の計画と実施における BCM の関与の度合いを示しています。本年の調査では、66% の企業がこの関与を「非常に重要である」と評価しています。29% は、BCM の関与を「重要である」と評価しています。昨年の調査では、63% と 31% がそれぞれ、BCM の関与を「非常に重要である」、「重要である」と評価しました。

**図 6. インシデント対応プロセスに対する BCM の貢献をどのように評価していますか?**
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)



**BCM は、情報漏えいの 1 件当たりのコストを削減します。**図 7 は、インシデント対応の計画と実施に BCM チームを関与させている企業と関与させていない企業における 3 年間の情報漏えいの 1 件当たりの平均コストを示しています。BCM を関与させている企業の方が、BCM を関与させていない企業よりも 1 件当たりのコストが低くなっています。本年の調査では、BCM を関与させている企業と関与させていない企業の間の情報漏えいの 1 件当たりのコストの差は ± 9 ドルです。割合の差は 11% です。

**図 7. BCM を関与させた企業と関与させなかった企業の情報漏えいの 1 件当たりのコスト**
割合の差 (2016 年 = 11%、2015 年 = 9%、2014 年 = 13%)
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)

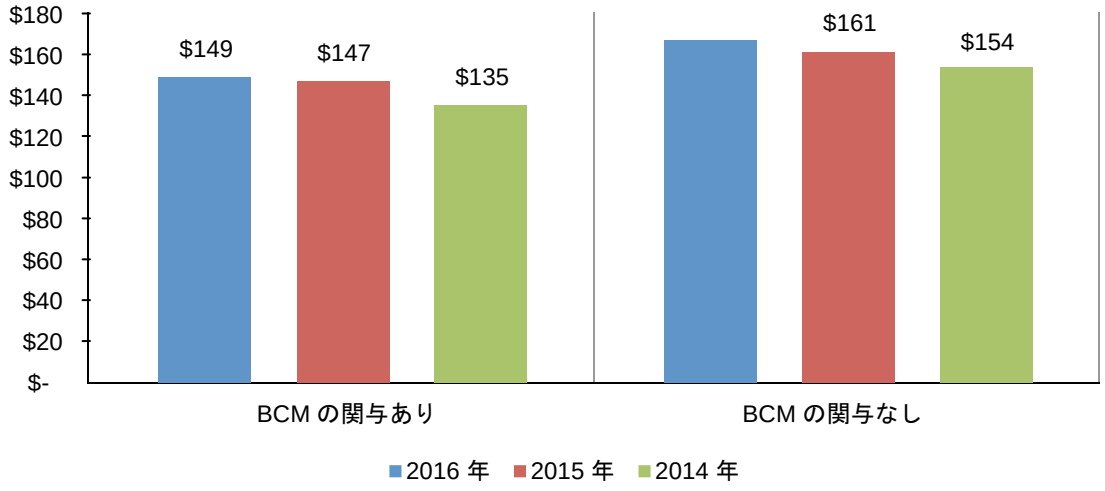
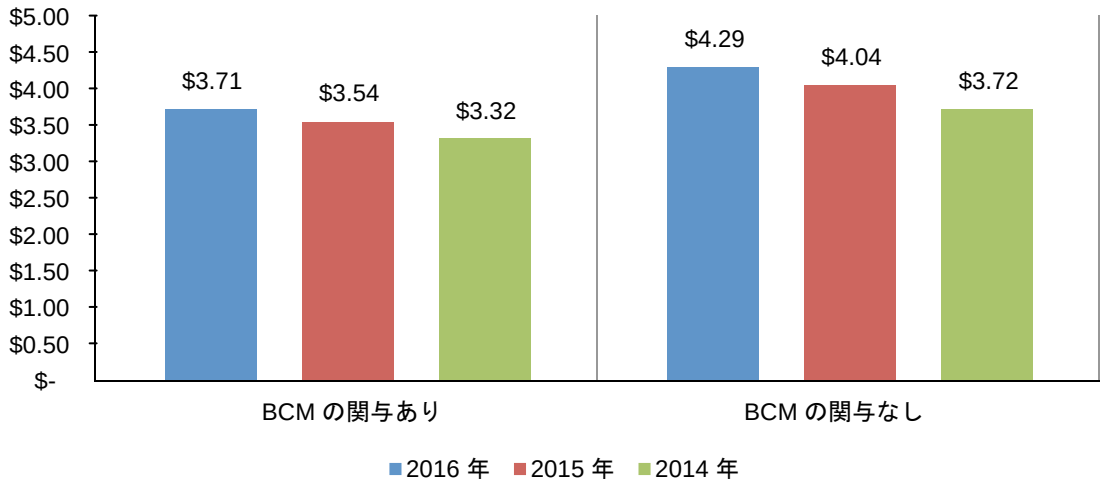



図 8 は、インシデント対応の計画と実施に BCM チームを関与させている企業と関与させていない企業における 3 年間の情報漏えい時に発生する総コストを示しています。上記と同様、BCM を関与させている企業の方が、BCM を関与させていない企業よりも情報漏えい時に発生する総コストが低くなっています。本年の調査では、BCM を関与させている企業と関与させていない企業の総コストの差は 580,000 ドルを超えました。割合の差は 15% でした。

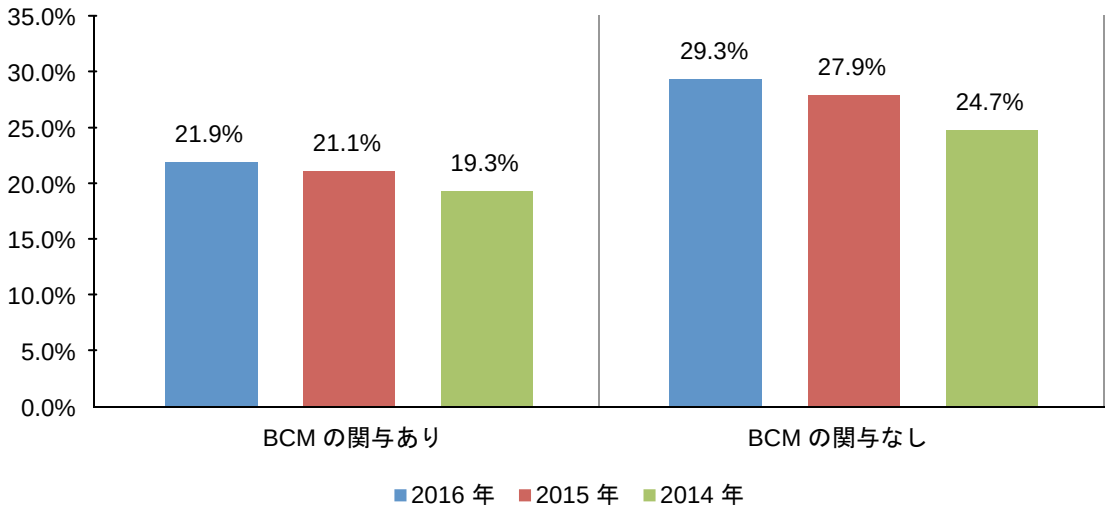
**図 8. BCM を関与させた企業と関与させなかった企業の情報漏えいの総コスト**
割合の差 (2016 年 = 15%、2015 年 = 13%、2014 年 = 11%)
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)
(百万ドル)



**BCM は情報漏えいの発生確率を削減します。**図 9 は、BCM を関与させている企業と関与させていない企業で今後 24 カ月間に 10,000 件以上のレコードの情報漏えいが発生する平均確率を示しています。

過去 3 年間において、BCM チームを関与させている企業の方が、BCM を関与させていない企業よりも発生確率が低いことが明らかになっています。本年の調査では、BCM を関与させている企業と関与させていない企業の間の今後情報漏えいが発生する確率の差は 29% でした。

**図 9. BCM を関与させている企業と関与させていない企業で重大な情報漏えいが発生する確率**
割合の差 (2016 年 = 29%、2015 年 = 28%、2014 年 = 25%)
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)

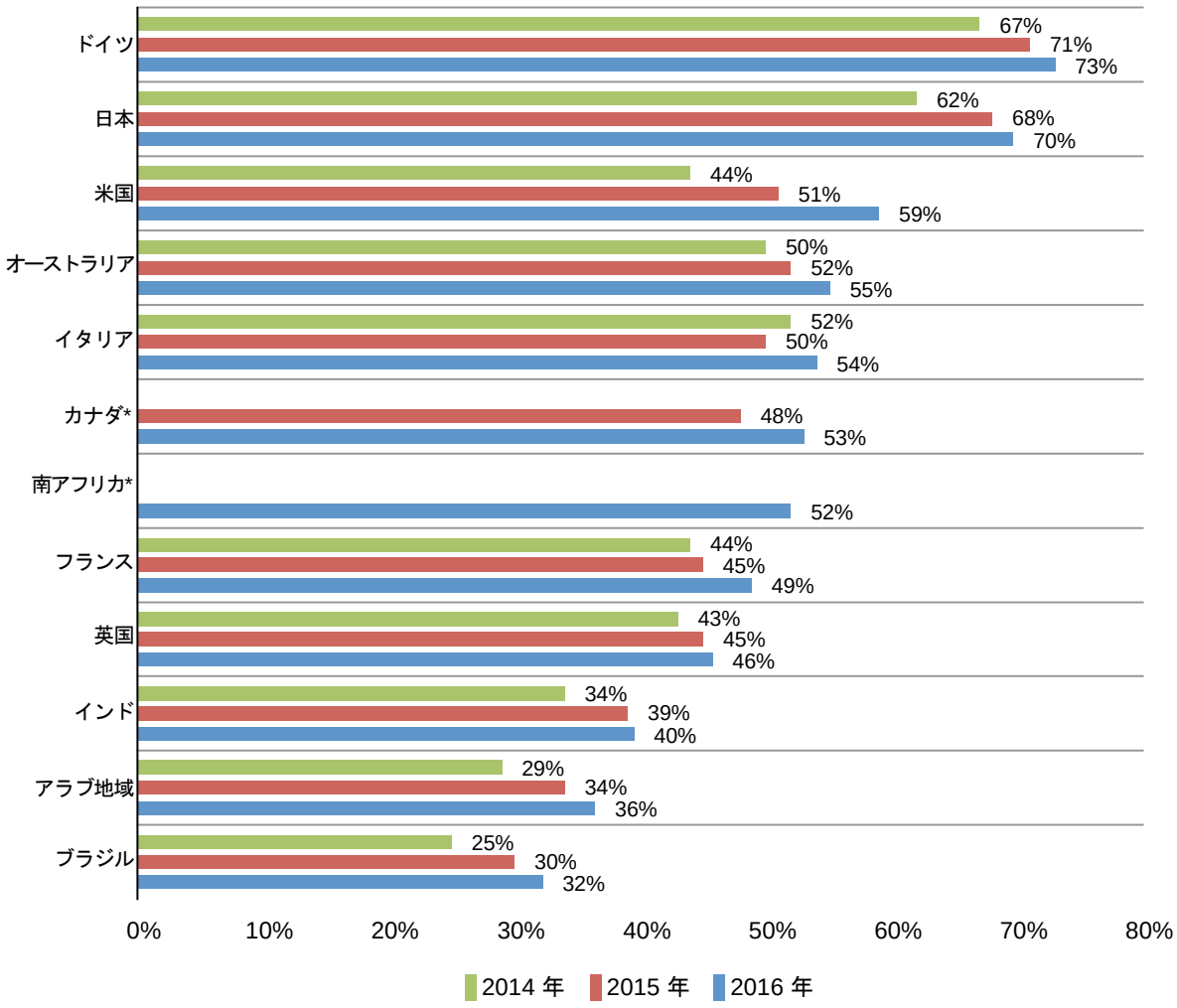


**情報漏えいに対処するときに BCM を関与させる可能性が最も高いのはドイツと日本です。**図 10 は、12 カ国のサンプルにおけるインシデント対応の計画と実施への BCM チームの関与の割合を示しています。過去 3 年間と同様、BCM が関与する割合が最も高いのはドイツ (DE) でした。ドイツの企業の 73% が BCM チームが存在していると報告しています。対照的に、BCM を関与させているブラジル (BZ) の企業はわずか 32% でした。注目すべき点として、すべての国で過去 1 年間に BCM の関与が高くなっています。

**図 10. 国のサンプル別の BCM の関与の割合**

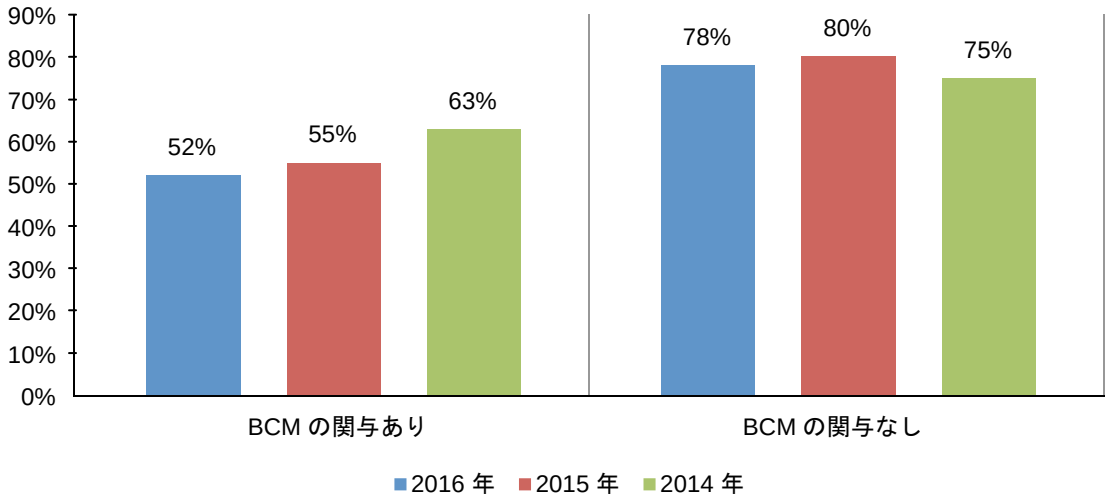
*履歴データなし

対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)



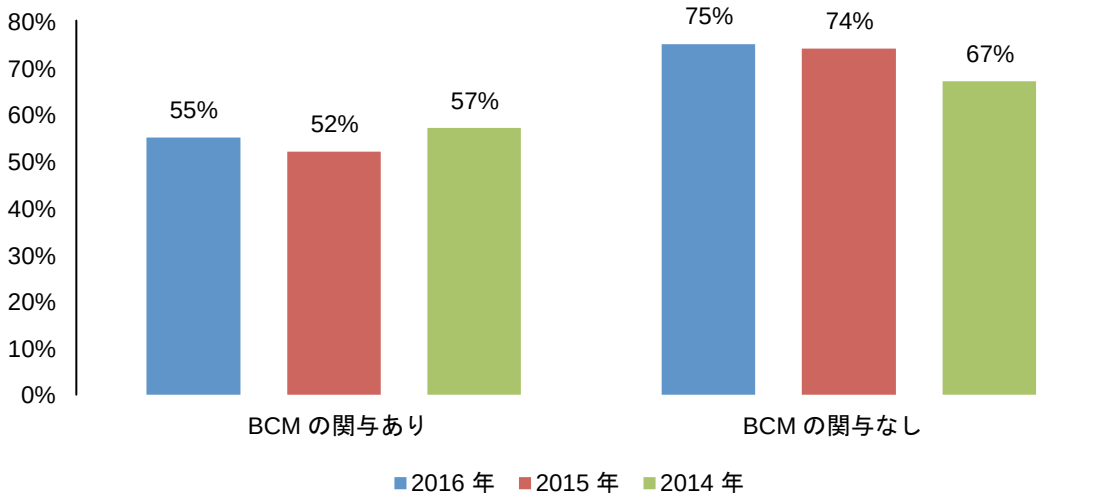
**BCM は、情報漏えいが発生した場合の事業運営の中断を最小限に抑える。**図 11 は、BCM を関与させている企業と関与させていない企業でのビジネス・プロセスの重大な中断に関する違いを明らかにしたものです。2016 年の報告によると、BCM を関与させていない企業の 78% が、情報漏えいインシデントが原因でビジネス・プロセスに重大な中断が発生したと報告しています。一方、BCM を関与させている企業のうち、重大な中断が発生したと報告したのは 52% でした。3 年間を通して、同様のパターンが当てはまります。

**図 11. 情報漏えいが原因でビジネス・プロセスに重大な中断が発生したことがありますか?**
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)




**BCM の関与により、IT 運用のレジリエンスが改善される。**上記と同様に、図 12 は、BCM を関与させている企業と関与させていない企業での IT 運用の重大な中断に関する違いを示しています。2016 年の報告によると、BCM を関与させていない企業の 75% が、情報漏えいインシデントが原因で IT 運用に重大な中断が発生したと報告しています。対照的に、BCM を関与させている企業のうち、インシデントによって重大な中断が発生したと報告したのは 55% でした。過去 2 年間にも同様のパターンが当てはまります。

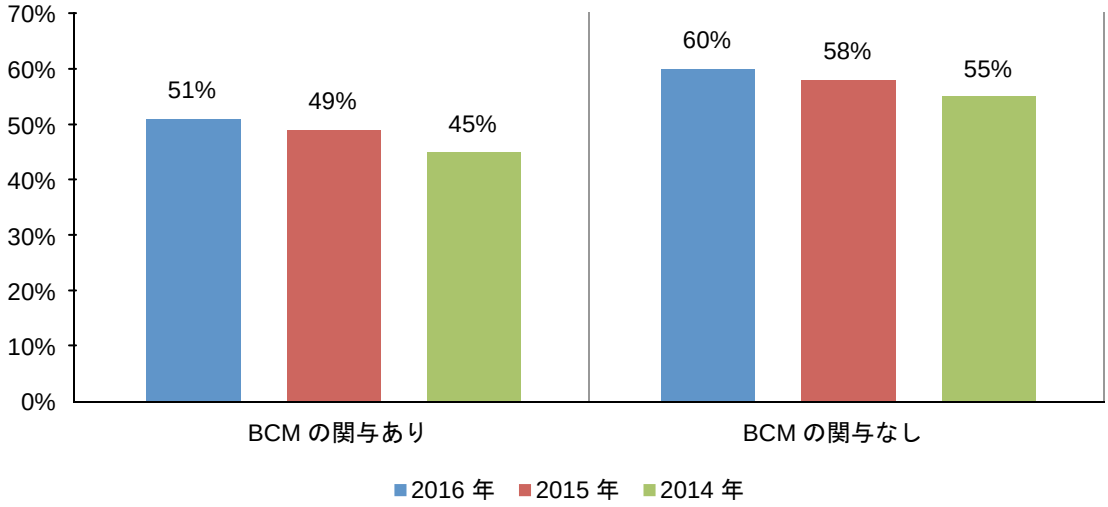
**図 12. 情報漏えいインシデントが原因で IT 運用に重大な中断が発生したことがありますか?**
対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)



**BCM は情報漏えい発生後の企業評価を保護できる。**図 13 は、BCM を関与させている企業と関与させていない企業の違いを示しています。本年の調査では、BCM を関与させていない企業の 60% が、情報漏えいが企業の評価、ブランド、市場におけるイメージに深刻な悪影響を与えたと報告しています。対照的に、BCM を関与させている企業のうち、インシデントが企業の評判やブランドに悪影響を与えたと報告したのは 51% でした。2015 年と 2014 年も同様のパターンが当てはまりました。

**図 13. 情報漏えいは企業評価に深刻な悪影響を与えましたか?**

対象: 全企業 (2016 年 = 383 社、2015 年 = 350 社、2014 年 = 315 社)



## 第 3 部: 情報漏えい時に発生するコストの計算方法

情報漏えい時に発生するコストの算出には、活動基準原価計算 (ABC) と呼ばれるコスト計算方法を使用しました。この方法では、業務を特定し、実際に投入されたコストを割り当てます。
今回のベンチマーク調査対象企業には、情報漏えいの問題解決で発生するすべての業務のコストの概算を依頼しました。

情報漏えいを検出するための業務と、情報漏えいの直後の対応として、一般的に以下が挙げられます。

- 調査と分析を実施して、情報漏えいの根本原因を判断する
- 情報漏えいの被害者を推定する
- インシデント対応チームを編成する
- コミュニケーション活動を実施して、広報部門を通して周知する
- 報告書とその他の必要な情報開示文書を準備し、情報漏えいの被害者と管轄当局に報告する
- コール・センターの対応手順を作成し、専用のトレーニングを実施する

情報漏えいを検出した後は、一般的に以下の業務を実施します。

- 監査業務とコンサルティング業務
- 情報保護のための法的業務
- コンプライアンスのための法的業務
- 情報漏えいの被害者への無料または割引のサービス
- 個人情報保護業務
- 解約数や流出数に基づく対顧客の機会損失
- 顧客獲得とロイヤルティー・プログラムのコスト

上記の業務のコスト範囲を各企業に概算していただいた後、次に示す定義に従って、これらのコストを直接コスト、間接コスト、機会損失コストに分類しました。

- *直接コスト* – 特定の業務を実施する際に直接発生した費用。
- *間接コスト* – 投入された時間、労力、その他の企業リソースの金額のうち、直接コストに分類されない費用。
- *機会損失コスト* – 情報漏えいを被害者に報告した (およびメディアに公開した) 後に評判が低下した結果失われたビジネスの機会の費用

さらに、情報漏えいの検出、対応、被害拡散防止、是正措置といった取り組みのコスト要因となる、コア・プロセス関連業務も調査しました。これらの業務のコストは、『主な調査結果』セクション (第 2 部) で紹介しています。次の 4 つのコスト・センターがあります。

- 検出または発見: (保存中または) 移動中の個人情報の漏えいリスクがあることを合理的に検出するための業務です。
- エスカレーション: 保護されている情報が漏えいしたことを、定められた期限内に適切な担当者に知らせるための業務です。
- 通知: 企業が個人情報の紛失または盗難を、文書、電話、電子メール、不特定多数への情報開示によって漏えいの対象者に通知する業務です。
- 事後対応: 被害拡大を最小限に抑えるための追加の質問や推奨事項の問い合わせの手段を情報漏えいの被害者に提供する業務です。クレジット・レポートの監視や新規アカウント (新規クレジット・カード) の再発行も情報漏えいの事後対応に含まれます。

大部分の企業では、上記のプロセス関連の業務に加えて、情報漏えいインシデントに伴う機会損失コストが発生します。これは、既存顧客と見込み顧客による信用や信頼の低下が原因です。つまり、今回実施した調査から、情報漏えいインシデントによるマイナス宣伝効果が企業の評価に悪影響を与え、異常流出率や異常解約率の増加、さらには新規顧客獲得率の低下が発生することが分かります。

こうした機会損失コストの試算では、調査対象企業ごとに定義した平均的な顧客の「生涯価値」に基づくコスト評価方法が使用されます。

- 既存顧客の流出率: 情報漏えいインシデントの発生に伴い顧客関係を終了させる可能性が最も高い顧客の推定数です。顧客数の減少分は、情報漏えいインシデントが原因とする異常流出を示します。この数値は、ベンチマーク調査の聞き取り過程で経営陣が示した概算値に基づき、年率で表されます。[5]

- 新規顧客獲得の減少率: 情報漏えいインシデントの発生に伴い顧客関係の開始を忌避するターゲット顧客の推定数です。この数値は年率で表されます。

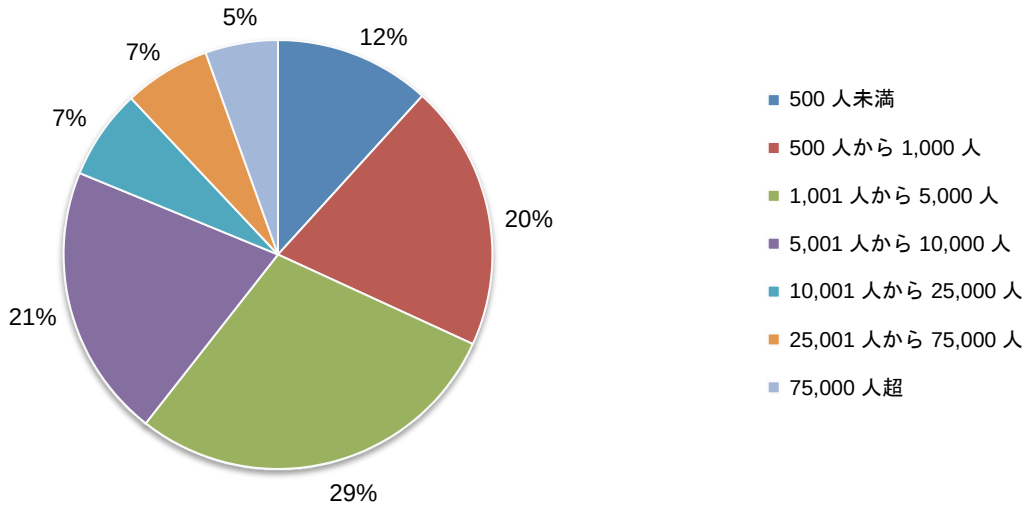
社員レコードなど顧客以外のデータの紛失は、顧客の解約や流出につながらない場合があることが確認されています。[6]
そのため、漏えいした情報に顧客データや利用者データ (支払取引に関する情報を含む) が含まれない場合、ビジネスの機会損失に分類されるコストは低くなると考えられます。

[5]場合によっては、流出が部分的なものにとどまることがあります。この場合、情報漏えいの被害者は企業との顧客関係を継続しますが、顧客としての活動量は以前に比べて低下します。この部分的な活動量の低下は、顧客関係の終了にコストが掛かりすぎたり、経済的な理由で顧客が関係を終了できないような、金融サービスや公共部門などの業種に多く発生します。

[6]この調査では、市民情報、患者情報、学生情報を顧客データとしています

円グラフ 3 は、ベンチマーク対象の企業の内訳を、総従業員数別に示したものです。最も多くを占めるのは、従業員数が 1,000 人を超える企業です。

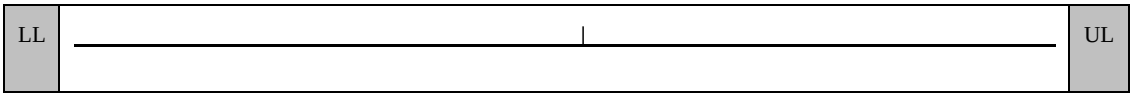
**円グラフ 4. 調査対象企業のグローバルな従業員数**
対象: 全企業 (n=383)




データ収集では、実際の会計情報は対象とせず、調査回答者の知識と経験から導き出された推定額を使う手法を採用しました。カテゴリーごとに、2 段階のコスト推定プロセスを実施しました。まず、ベンチマーク用の文書を使い、次のような数直線形式に可変のマークを設定して、コスト・カテゴリーごとに直接コストの概算を記入するよう依頼します。

数直線の使用法: 情報漏えい時に発生するコスト・カテゴリーごとに設定された数直線を使用して、発生した現金支出、人件費、その他の諸経費の合計について、最も近いと思われる推定額を入力します。設定された上限と下限の間に点を 1 つだけ付けてください。数直線の上限と下限は聞き取り中にいつでもリセットできます。

**[提示されたコスト・カテゴリー] の直接コストの推定額を記入してください。**




カテゴリーごとに具体的な推定額を 1 つ記入してもらう代わりに、数直線に基づいて数値を取得することで、情報の機密性が保たれ、回答率も高くなります。ベンチマーク文書の次の段階では、間接コストと機会損失コストの推定値を入力するよう調査回答者に依頼しました。

ベンチマークでは、プロセスが煩雑にならないよう、情報漏えい時に発生するコスト評価に欠かせないと判断した業務のコスト・センターだけを慎重に選び、対象項目に設定しました。経験豊富なエキスパートとの協議を通して、必要なコスト関連業務を含む一連の項目が最終決定されました。ベンチマーク情報の収集では、一貫性と包括性を保つため、各文書が繰り返し検証されました。

完全な情報機密を実現するため、ベンチマーク文書では企業が特定できるような情報を一切収集していません。説明資料でも、回答と調査対象企業がひも付けられるような、追跡番号やその他の情報を一切追加していません。

個人情報の取り扱いを伴う幅広い業務運用に対応するよう、ベンチマーク文書に記載された情報漏えい時に発生するコスト項目の範囲は、一般的に知られているコスト・カテゴリーだけに限定されています。今回の調査では、データ保護業務や個人情報のコンプライアンス業務を対象とせず、ビジネス・プロセス関連業務だけに注目したことで、高品質な結果が得られたと確信しています。

## 第 5 部: 制限事項

この調査では、前回の調査で問題なく実施できることが確認された、機密かつ独自のベンチマーク手法が使用されています。同時に、このベンチマーク調査には回避できない制限事項があります。本調査結果から結論を導き出す際は、次に示す制限事項について慎重に検討してください。

- 結果が非統計的: 今回の調査の基になったのは、非統計的な代表サンプルです。具体的には、過去 12 カ月間で顧客レコードまたは利用者レコードの紛失または盗難を伴う情報漏えいを経験した、世界中の企業です。非科学的なサンプリング手法のため、統計的推論、許容誤差、信頼区間をこれらのデータに適用することはできません。

- 無回答の存在: 今回得られた結果のベースとなるのは、少数の代表サンプルによるベンチマークです。このグローバル調査では、350 の企業がベンチマーク・プロセスを完了しました。ただし、無回答のバイアスはテストされていません。このため、まったく異なる情報漏えい時に発生するコストの傾向を非回答企業が有している可能性が常に存在します。

- サンプリング・フレームのバイアス: サンプリング・フレームは独自の判断で決定されているため、今回のサンプリング・フレームが調査対象企業の母集団をどの程度反映しているかによって、結果の品質は変化します。今回のサンプリング・フレームは、個人情報保護や情報セキュリティーの取り組みが一定以上進んでいる企業に偏っていると判断しています。

- 企業固有の情報: ベンチマークの情報は機密情報であり社外秘です。このため、今回の文書では企業を特定できるような情報は収集していません。回答者には、カテゴリー別の回答変数を使用した企業および業種についての属性情報の開示を許可しています。

- 調査対象外の要因: 聞き取り調査のスクリプトを簡潔かつ的を得たものにするために、主流のトレンドや企業の性格といった重要な可変要素は分析から除外されています。除外された可変要素がベンチマーク結果に与え得る影響は特定できません。

- 推定に基づくコスト結果: ベンチマーク調査の品質を支えているのは、調査対象企業の回答者が誰にも見られずに提供した回答の完全性です。ベンチマーク・プロセスに一定のチェック・アンド・バランスを適用することも可能ですが、回答者が不正確または不誠実に回答している可能性は常に存在します。また、実際のコスト・データではなくコスト推定の手法が採用されているため、何らかの事情で偏った結果や不正確な結果が推定されている可能性もあります。

本調査レポートに関するご質問やご意見をお寄せいただく場合、または本書の追加コピーが必要な場合 (本レポートの引用や再利用の許諾申請を含む) は、手紙、電話、電子メールのいずれかでお問い合わせください。

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

**www.ibm.com/security/data-breach** にて、すべてのレポートを提供しています。

## Ponemon Institute

***情報管理の信頼性向上に向けた取り組み***

Ponemon Institute は、独自の調査と教育を通して、企業と政府機関における信頼性に優れた情報管理と個人情報管理の実践を推進しています。当社のミッションは、ユーザーと企業の機密情報の管理と保護を左右するさまざまな重要課題に対して、豊富な経験を活かした高品質な調査を実施することです。

当社は、**Council of American Survey Research Organizations (CASRO)** の参加企業として、データの機密保持、個人情報保護、倫理に関する厳格な基準を遵守して調査活動を遂行しています。当社は、個人が特定できるようないかなる情報も収集しません (企業調査の場合は、企業が特定できるようないかなる情報も収集しません)。また、調査対象者に無関係な質問や不適切な質問をしないための厳格な品質基準を遵守しています。