損保ジャパン
SOMPO Innovation for Wellbeing

2020年４月1日

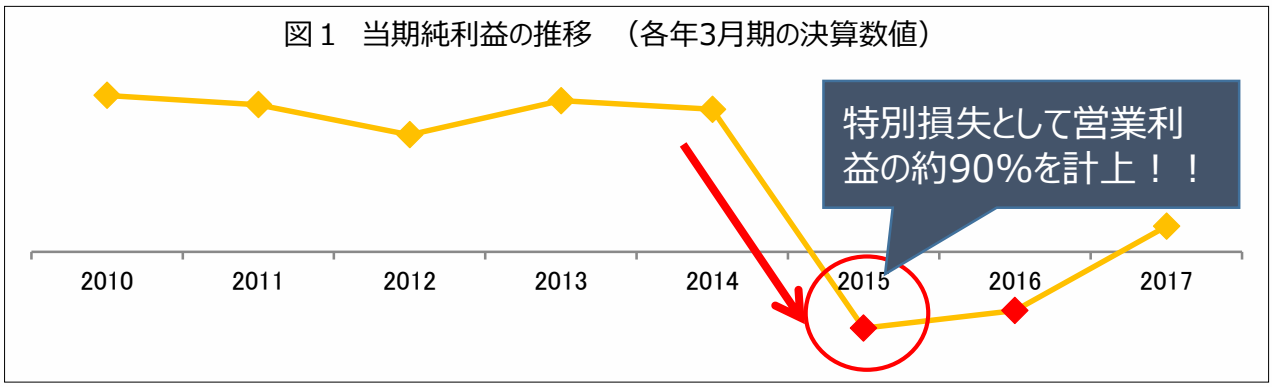
情報漏えいリスク、しっかり対策されていますか！？

個人情報漏えいによる経営への影響例

2014年に個人情報漏えいが発生したA社の業績推移

（１） 2014年の個人情報漏えい事故により赤字転落

図１ 当期純利益の推移 （各年3月期の決算数値）



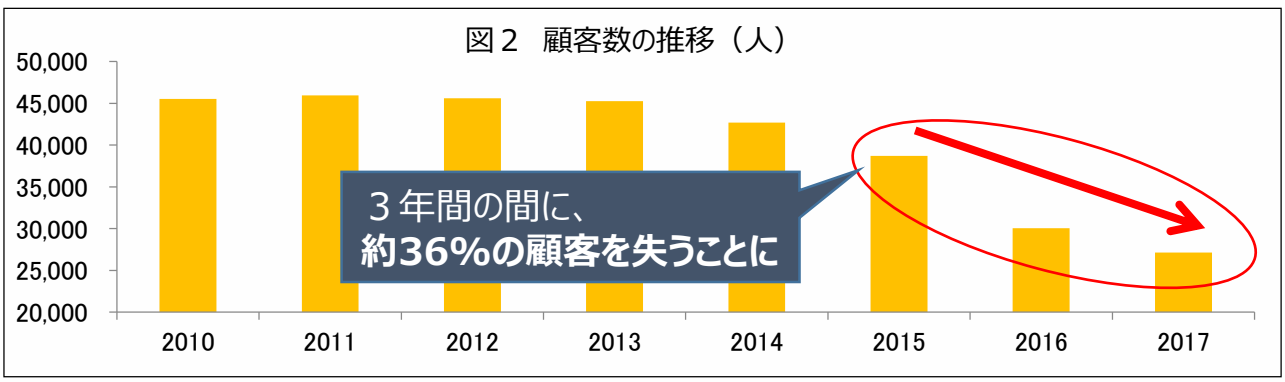
特別損失として計上された各種費用とは

Check Point

- ✓ 漏えい事故発生に関する原因調査費用
- ✓ 情報漏えいの顧客に対するお詫び対応（見舞品など）、訴訟対応費用
- ✓ 再発防止のための情報セキュリティ対策費 など

（２） **営業利益も18.4%の減益** その要因は顧客からの信頼失墜！？

図２ 顧客数の推移（人）



事故発生時に適切な対応ができず、業績への影響は長期間に・・・

Check Point

ブランド維持のためのポイントは、
- ✓ 個人情報発生後の**適切な**情報公開
- ✓ 情報漏えいした顧客への**適切な**お詫び対応（見舞品など）

実際に情報漏えいが発生する原因と、発生後の対策は裏面で！

避けられない　情報漏えい・サイバー攻撃被害

一般企業で発生した情報漏えい・サイバー攻撃の事件・事故種類

※　（）内の数字は、回答企業1794社のうちアンケート期間（2019年1月-2月）以前1年間に調査該当事故が発生した割合

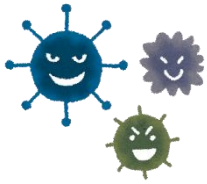
電子メール、FAX、郵便物等の誤送信・誤配送
（　２９.４％　）

情報機器・外部記憶媒体等の紛失・置き忘れ
（　２２.６％　）

【事故事例】
社員が出張中に、ノートパソコンを鞄ごと盗難された。パソコンに保存されていた顧客の個人情報（氏名、電話番号、メールアドレス、銀行口座）3,000件が流出。

マルウェア感染（コンピューターウイルス）
（　２２.５％　）

【事故事例】
標的型メール（※）による被害
職員がメールに添付されているファイルを開封した際にPCがマルウェアに感染。このPC経由で社内システムから情報を抜き取られ、顧客情報1万件が流出。



※標的型メール　：　注文を装った注文書添付のメールや製品の問い合わせ、システム管理会社からの注意喚起メールになりすまして、添付ファイルを開かせマルウェア感染させる手法です。

出典：NRIセキュアテクノロジーズ『企業における情報セキュリティ実態調査2019 』

自信のある企業さまはぜひ、当社担当まで無料診断サービスのご依頼を！！

- **”お試し版”標的型攻撃メール対応訓練**
- **サイバーリスク簡易診断・プラスサービス**

損保ジャパンではサイバー保険を通じて、事故発生時の高額な対応費用と顧客の信頼回復への総合的なサポートを提供します！

	想定されるリスク	事故後に必要な対応	損保ジャパンのサポート
サイバー攻撃	■ マルウェア感染によるシステム停止および業務中断 ■ 不正アクセスによる顧客情報の漏えい など	● 原因究明調査 ● システム復旧・業務再開 ● 有事広報（記者会見・広告・お詫び文） ● 専用コールセンターの立上げ・運用 ● 再発防止策・信頼回復策の検討・公表 ● 損害賠償請求時の応訴	**① 保険金によるファイナンス機能** **（賠償金・各種費用の支払い）** **② 緊急時の総合的な対応サポート** **原因究明やコンサルティングにかかる費用など**
内部不正による情報漏えい	■ 委託先・内部犯行による名簿業者への転売 など		
物理的要因による情報漏えい	■ 書面紛失、委託者のずさんな管理による情報漏えい など		

●このちらしは概要を説明したものです。詳しい内容につきましては取扱代理店または損保ジャパンまでお問い合わせください。

損害保険ジャパン株式会社
SOMPO

〒160-8338　東京都新宿区西新宿1-26-1
＜連絡先＞https://www.sompo-japan.co.jp/contact/

＜お問い合わせ先＞

(SJNK19-50260)　　2019年７月29日作成