NAD MonthlyReport.

MarketFlash

サイバーリスクマネージメント　No2
～情報セキュリティ対策～

2018.7&8

日本アルプス電子株式会社
NIHON ALPS ELECTRONICS CO.,LTD.

暑中お見舞い申し上げます

平素は格別のお引き立てにあずかり、誠にありがとうございます。

連日の酷暑ですが、くれぐれもご自愛のほどお祈り申し上げます。

今後共なお一層ご愛顧のほどよろしくお願い申し上げます。

サイバーリスクマネージメント
情報セキュリティインシデント調査結果2016

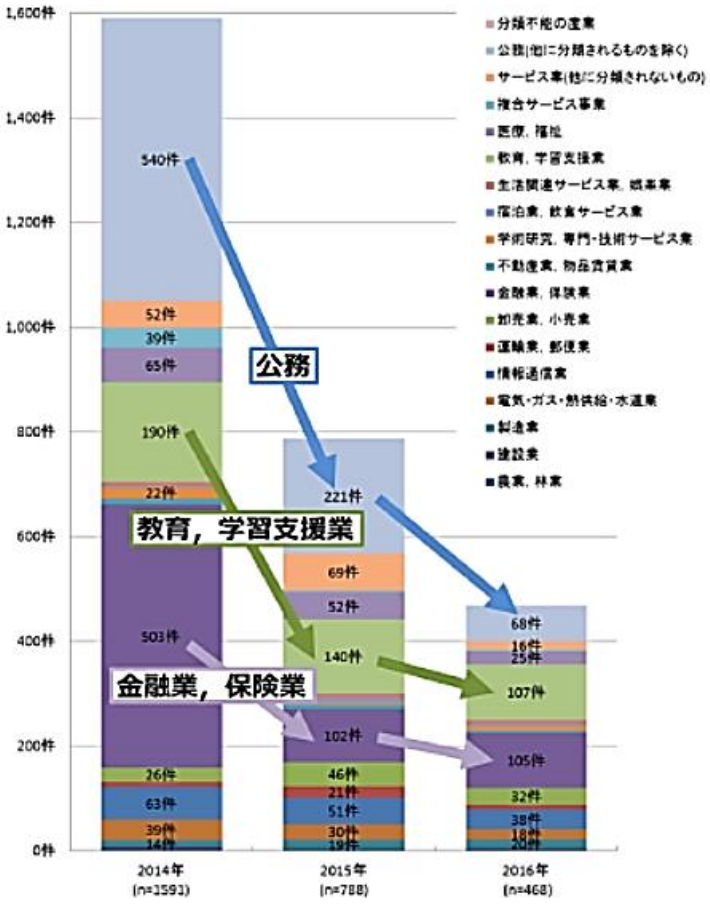

図 1-1：業種別インシデント件数（経年）

日本ネットワークセキュリティ協会による個人情報漏洩に関するインシデント調査（2016年）結果

インターネットから収集できた2016年の個人情報漏洩インシデントの件数は、大きく減少している。過去の調査結果と比較して、特に漏洩人数が1～10人規模のインシデント件数の減少が顕著である。この要因としては、これらの規模のインシデントを公表しなくなったということが考えられる。インシデントを公表しなくなった要因は、インシデント1件当たりの漏洩人数が少ないことや漏洩した個人情報が暗号化されていた、もしくは機微な情報が洩れていない場合は、公表不要とするようになったと思われる。

経路別のインシデント件数をみると、紙媒体のインシデント件数が大きく減っている。USB等可搬記録媒体からのインシデント件数も減少傾向になる。半面、インターネット経由の個人情報漏洩は減少していない。インターネット上では新しい攻撃が次々と発生しているため、他の媒体と比べてインシデントが発生するリスクが高いと想定される。

個人情報漏洩については、これまで数多くの新市電とが発生し社会問題にもなってきていることから、中小企業においても個人情報漏洩に関する社内規定が整備され、個人情報の管理体制が確立してきていることから、これらのデータで見るように件数的には減少してきている傾向にある。
ただ、その内容を見ると、社内管理が厳しくなったことから、人的ミス（データの持ち出しによる紛失など）が減少したことが大きな要因となっている。
これからは、インターネット経由での個人情報漏洩をいかに防ぐかが重要な課題となっている。

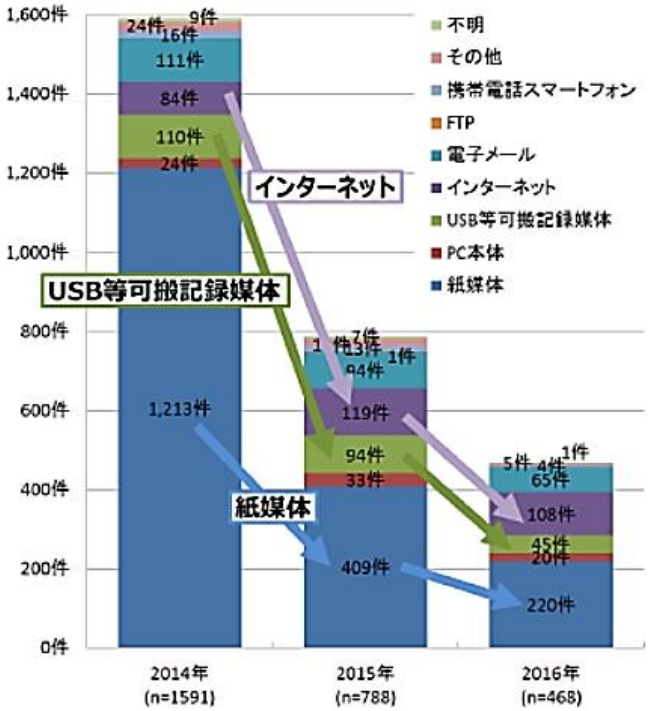

図 1-2：漏えい経路別インシデント件数（経年）

サイバーリスクマネージメント
情報セキュリティインシデント調査結果2016

2016年インシデント分析概要

漏洩件数は、468件（前年比320件減少）であった。2014年から減少傾向であるが、近年は軽微な個人情報漏洩インシデントの公表が減っているため、件数が少ない。

漏洩人数は、約1,397万人（前年比901万人増）と大幅に増加。想定損害賠償総額は、約2994億円（前年比262億円増）となった。大規模なインシデントが1件発生（JTB680万件の流出）したためである。

漏洩原因は、「管理ミス」が一番多く、「誤操作」「不正サクセス」の3種類が全体の64%を占めた。

表 4-1：2016 年 個人情報漏えいインシデント 概要データ

漏えい人数	1,396 万 5,227 人
インシデント件数	468 件
想定損害賠償総額	2,788 億 7,979 万円
一件あたりの漏えい人数※1	3 万 1,453 人
一件あたり平均想定損害賠償額※1	6 億 2,811 万円
一人あたり平均想定損害賠償額※2	3 万 1,646 円

表 4-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	679 万人	生活関連サービス業，娯楽業	ワーム・ウイルス
2	98 万人	情報通信業	不正アクセス
3	81 万人	電気・ガス・熱供給・水道業	紛失・置忘れ
4	64 万人	情報通信業	不正アクセス
5	58 万 9463 人	情報通信業	不正アクセス
6	42 万 8138 人	情報通信業	不正アクセス
7	42 万 1313 人	卸売業，小売業	不正アクセス
8	35 万人	生活関連サービス業，娯楽業	不正アクセス
9	21 万 9025 人	卸売業，小売業	不正アクセス
10	21 万人	電気・ガス・熱供給・水道業	管理ミス

サイバーリスクマネージメント
情報セキュリティインシデント調査結果2016

個人情報インシデントの過去の推移データ

2005年からの推移データは以下の通りである。
2014年はベネッセによる約3500万人のデータ流出、2016年はJTBによる約680万人のデータ流出が発生しているため大きく増加している。
しかし、管理体制が厳格になってきているにもかかわらず、個人情報漏洩は減少傾向にはないということは大きな問題である。
また、こうした個人情報漏洩以外のサイバー攻撃によるインシデントの発生は確実に増加傾向にある。サイバー攻撃による損害は、個人情報漏洩に限らず、企業活動そのものに損害を与えるものであり、その損害は膨大である。

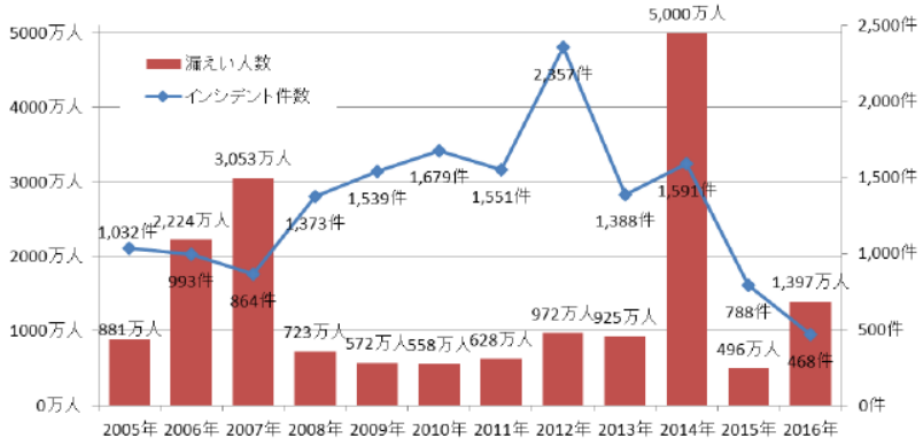

図 4-29：インシデント件数と漏えい人数の経年変化（合計）

表 5-1：想定損害賠償総額の経年変化

	想定損害賠償総額
2005 年	約 5,329 億円
2006 年	約 4,570 億円
2007 年	約 2 兆 2,711 億円
2008 年	約 2,367 億円
2009 年	約 3,890 億円
2010 年	約 1,215 億円
2011 年	約 1,900 億円
2012 年	約 2,133 億円
2013 年	約 1,439 億円
2014 年	約 1 兆 6,642 億円
2015 年	約 2,527 億円
2016 年	約 2,789 億円

表 5-2：一人あたりの平均想定損害賠償額

	想定損害賠償総額
2005 年	4 万 547 円
2006 年	3 万 6,743 円
2007 年	3 万 8,228 円
2008 年	4 万 3,632 円
2009 年	4 万 9,961 円
2010 年	4 万 2,662 円
2011 年	4 万 8,560 円
2012 年	4 万 4,628 円
2013 年	2 万 7,675 円
2014 年	5 万 2,625 円
2015 年	3 万 4,058 円
2016 年	3 万 1,646 円

表 5-3：一件あたりの平均損害賠償額の経年変化

	一件あたりの 平均想定損害賠償額	(参考) 想定損害賠償総額
2005 年	5 億 3,935 万円	約 5,329 億円
2006 年	4 億 8,156 万円	約 4,570 億円
2007 年	27 億 9,347 万円	約 2 兆 2,711 億円
2008 年	1 億 8,552 万円	約 2,367 億円
2009 年	2 億 6,683 万円	約 3,890 億円
2010 年	7,551 万円	約 1,215 億円
2011 年	1 億 2,810 万円	約 1,900 億円
2012 年	9,313 万円	約 2,133 億円
2013 年	1 億 6,575 万円	約 1,439 億円
2014 年	10 億 8,561 万円	約 1 兆 6,642 億円
2015 年	3 億 2,192 万円	約 2,527 億円
2016 年	6 億 2,811 万円	約 2,789 億円

サイバーリスクマネージメント
情報セキュリティ対策

先月のレポートからサイバーリスクについての具体的な内容についてみてきましたが、ここからはその対策についてまとめてみた。
企業での情報セキュリティ対策としてどのようなことが求められているのでしょうか？
独立行政法人情報処理推進機構の「中小企業の情報セキュリティ対策ガイドライン」の概要をご紹介する。

1.経営者としての責任

法的責任としては、

- 個人情報やマイナンバーに関する違反の場合は刑事罰が科されます。また、その場合は個人情報保護委員会による立入検査を受ける責任もある。
- 民法上の不法行為とみなされた場合は、経営者が個人として損害賠償責任を負う場合もある。

社会的責任として、
情報漏えい事故は、営業機会の喪失、売上高の減少、企業のイメージダウンなど、自社に損失をもたらし、会社役員は会社法上の責任(会社に対する損害賠償責任)を負っているので、場合によっては株主代表訴訟を提起されることもあり得る。さらには、取引先との信頼関係の喪失、業界全体のイメージダウンにもなってしまう。したがって、情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすためにも重要である。

2.経営者が認識する必要のある「3原則」

(1)情報セキュリティ対策は経営者のリーダーシップで進める

セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

(2)委託先の情報セキュリティ対策まで考慮する

子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

(3)関係者との情報セキュリティに関するコミュニケーションは常に怠らない

ステークホルダー(顧客や株主等)の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

サイバーリスクマネージメント
情報セキュリティ対策

(2)経営者がやらなければならない「重要7項目の取組」

経営者は、以下の「重要7項目の取組」について、自ら実践するか、実際に情報資産や情報システムなどの管理を実践する管理者層に対して指示することで、確実に実施することが必要。

取組1 情報セキュリティに関する、組織全体の対応方針を定める

情報セキュリティ対策を組織的に実施する意思を、関係者に明確に示すために、情報セキュリティに関する方針を定め、要求に応じて提示できるようにする

- 「当社は中小企業の情報セキュリティ対策ガイドラインに基づき情報セキュリティ対策を実践する。」
- 「当社は顧客情報の流出防止を徹底することから情報セキュリティ対策を開始する。」

取組2 情報セキュリティ対策のための資源(予算、人材など)を確保する

情報セキュリティ対策を実施するために、必要な予算と人材を確保。これには万が一事故(インシデント)が起きてしまった場合、被害を最小限に止めるために、あらかじめ準備することも含む。

取組3 担当者に必要と考えられる対策を検討させて実行を指示する

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させる。検討した対策ごとに予算を与え、担当者を任命し、実行を指示。実施する対策は、社内ルールとして文書にまとめておけば、従業員も実行しやすくなり、取引先などにも取り組みを説明する際に役に立つので、併せて指示する。

取組4 情報セキュリティ対策に関する定期・随時の見直しを行う

情報セキュリティ対策を最初から最適な形で実現することはどんな会社でも難しい。また情報技術は進化が早く、加えて脅威も変化する。そのため、一度定めた対策がいつまでも有効であるとは限らないので、取組3で定めた情報セキュリティ対策について、定期または随時に見直して、必要な改善や追加の対策を決めるように担当者に指示する

取組5 業務委託や外部サービスを利用する場合は、情報セキュリティに関する責任範囲を明確にする

業務の一部を外部に委託(共同実施も含む)する場合は、相手先でも少なくとも自社と同等の対策が行われるようにしなければならない。そのためには契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する必要がある。また必要に応じて相手先を訪問し、対策の実施状況を確認する。

ITシステム(電子メール、ウェブサーバー、ファイルサーバー、業務アプリケーションなど)に関する技術に詳しい人材がいない場合には、外部サービスを利用したほうが、コストと情報セキュリティ対策との両面から有利なときがある。ただし、無償の外部サービスなど情報セキュリティ対策を求めることが難しい場合や、有償であっても個別契約等でサービス提供者の責任や対策を規定することが難しい場合もあるので、利用規約やサービスに付随する情報セキュリティ対策等を確認したうえで選定するよう担当者に指示する必要がある。

サイバーリスクマネージメント
情報セキュリティ対策

取組6　情報セキュリティに関する最新動向を収集する

情報技術の進化の早さから、脅威やその対策は目まぐるしく変化する。自社だけで全ての脅威や対策を把握することは困難なため、情報セキュリティに関する最新動向を発信している公的機関などを把握しておき、常時参照することで、新たな脅威に備えるようにする。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有する。

取組7　緊急時の社内外の連絡先や被害発生時の対処について準備しておく

情報セキュリティ対策を実施するとともに、万が一のインシデントに備えて、緊急時の連絡体制を整備。さらに、その連絡体制がうまく機能するかをチェックするためインシデントを想定した模擬訓練を定期的に行うと理想的である。一方、インシデントにより情報資産の漏えいなどの被害が出た場合には、情報資産の提供元や個人情報の本人などへの連絡も必要となることがあり、速やかに連絡可能なようにあらかじめ準備しておくとともに、経営者の対応についても、あらかじめ決めておけば、冷静で的確な対応が可能になる。

▲情報セキュリティに関する最新動向を発信している公的機関
IPA（独立行政法人情報処理推進機構）のウェブサイト
https://www.ipa.go.jp/security/index.html
NISC（内閣サイバーセキュリティセンター）のウェブサイト
http://www.nisc.go.jp/

サイバーリスクマネージメント
情報セキュリティ5か条

情報セキュリティ5か条

1. OSやソフトウェアは常に最新の状態にすること

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性がある。OSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにする。

- WindowsUpdate(WindowsOSの場合)/ソフトウェア・アップデート(macOSの場合)/OSバージョンアップ(Androidの場合)
- AdobeFlashPlayer/AdobeReader/Java実行環境(JRE)など利用中のソフトウェアを最新版にする

2. ウイルス対策ソフトを導入すること

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えている。ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態になるようにする。

- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)の導入を検討する

3. パスワードを強化すること

パスワードが推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増えている。パスワードは「長く」「複雑に」「使い回さない」ようにして強化すること。

- パスワードは英数字記号含めて10文字以上にする
- 名前や誕生日、簡単な英単語などはパスワードに使わない
- 同じパスワードをいろいろなウェブサービスで使い回さない

4. 共有設定を見直すこと

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため無関係な人に情報を覗き見られるトラブルが増えている。クラウドサービスや機器が、無関係な人に共有されていないか設定を確認すること。

- クラウドサービスの共有範囲を限定する
- ネットワーク接続のふくごうきやカメラ、ハードディスクなどの共有範囲を限定する
- 従業員の移動や退職時に設定の変更(削除)漏れがないように注意する

5. 脅威や攻撃の手口を知ること

取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧みな手口が増えている。脅威や攻撃の手口を知って対策を取るようにすること。

- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

サイバーリスクマネージメント
サイバー保険

最後に、このようなサイバー攻撃に対する対策を講じたとしても、サイバー攻撃の手口は日々進化しており、企業にとってどうしても防ぎきれないものである。

そうした部分については外部にリスク移転することも重要である。

経済産業省の「サイバーセキュリティ経営ガイドライン」の中でも以下のように、サイバー保険の利用を奨めている。

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。
その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

情報セキュリティに関するリスク及びその対策は今後企業経営の最重要課題となってくるであろう。
企業経営者は常に最新動向を把握し、その対策の見直しを常に行うことが重要である。

サイバー保険の特徴

特長1 包括的な補償
セキュリティ事故に起因して発生した各種損害を1つの保険で包括的に補償します。

特長2 不正アクセス等の“おそれ”の調査費用も補償
不正アクセス等の発見時の各種対応費用だけでなく、不正アクセス等の“おそれ”が発見された時の外部機関への調査依頼費用も補償します。

特長3 海外提起の損害賠償請求訴訟も補償
海外で提起された損害賠償請求訴訟についても補償します。

特長4 利益損害・営業継続費用も補償(オプション)
ネットワークの中断による自社の利益損害・営業継続費用についても補償します。

特長5 保険以外のサービスのご提供
「サイバーリスク総合支援サービス」がご利用いただけます。

東京海上日動のHPより一部抜粋