KDDI まとめてオフィス

NRI SECURE

NRIセキュア×KDDI まとめてオフィスの共同アンケートでわかった

中堅企業・中小企業のための セキュリティ対策を 進めるキーポイント

はじめに

大手企業、官公庁での情報漏えいなどのセキュリティ事故が報道されない年はないと言っていいかもしれない。そして、報道されるセキュリティ事故の背後には、報道されない事故、事故に至らないまでも事故一歩手前の「ヒヤリハット」の状況が数多くあることは想像に難くない。

そして、なにもセキュリティ事故は大企業だけのものではない。いまやITを利用せずに事業を行っている企業がない以上、ビジネスとセキュリティ事故は切っても切れない関係にある。

今回、KDDI まとめてオフィスとNRIセキュアテクノロジーズ（以下、NRIセキュア）は、共同で企業のセキュリティに関するアンケートを実施した。そこからは、企業セキュリティの実情と今後の取組へのヒントが見えてきた。

調査概要

調査実施時期：2018年7月30日～8月3日
調査方法　　：ウェブアンケート
調査対象者　：KDDI ビジネスメールマガジンをご購読のお客様
有効回答者数：1,778名

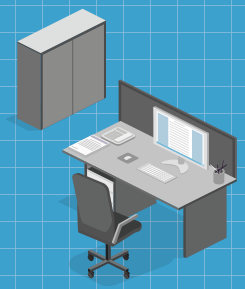
目　次

エグゼクティブサマリー …… 3
第１章　実情分析 …… 6
第２章　原因 …… 8
第３章　きっかけ …… 10
第４章　今後の取り組み …… 13

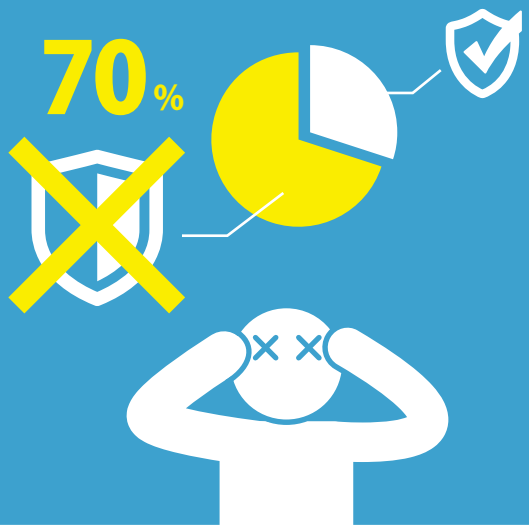
Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

アンケートで分かった

進まないセキュリティ対策の現状と課題



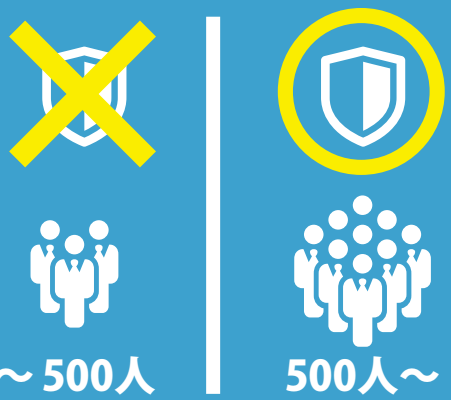
7割もの企業が
『セキュリティ対策が
十分でない』と回答



『事故がまだ
起こっていないから…』、
セキュリティ対策が進まない
のは『意識の低さ』が
最大の障壁になっている

法制度・取引条件など、
『外圧』があれば、
セキュリティ対策は進む

従業員500名の壁。
従業員数500名以上の
企業では、比較的、
セキュリティ対策が進んでいる
傾向がある

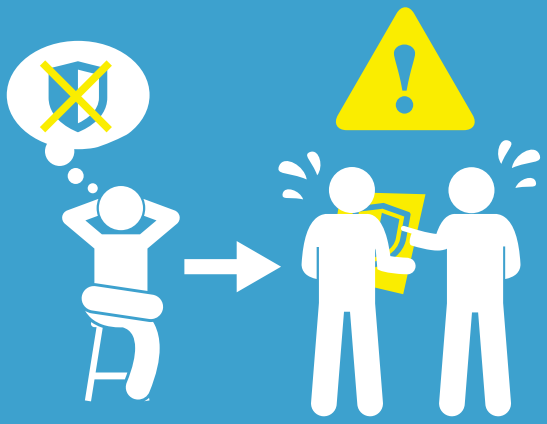


Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

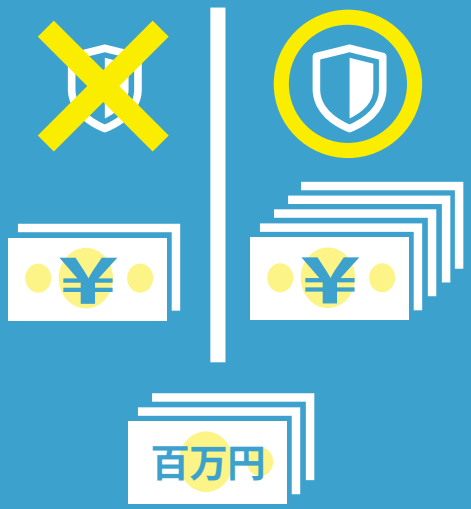
拠点数が増えると
高まるセキュリティ意識。
しかし、**拠点が増えていくと**
『目が行き届かなくなる』

『専門部署』の存在は
対策を進める

社内での
セキュリティ事故発生が
きっかけに。
『なにかが起こってから』しか
対策が進まない



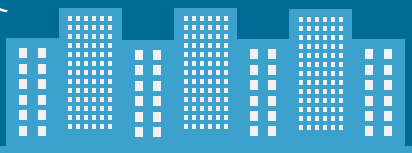
セキュリティ対策が
進んでいる企業は、
きちんと**予算を確保している？**

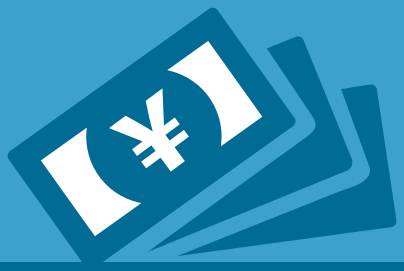


Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

セキュリティ対策が進んでいる企業の4つの特徴

アンケートからは、下記を満たす企業しか
十分なセキュリティ対策が行われていないという傾向だった。
しかし、**多額の予算をかけなくても、企業規模が小さくても、**
セキュリティ対策が十分にできている企業は存在する。
その違いをアンケート結果を分析することで
紐解いていきたい。

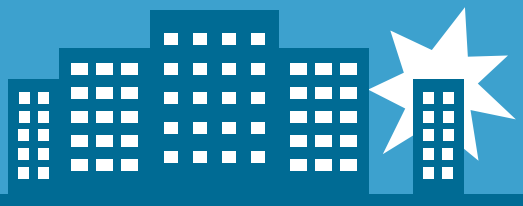




セキュリティ予算※を適切に確保

※セキュリティ対策への新規投資や運用・管理費用等も含むセキュリティ対策全般にかかるコスト

従業員数500名以上



取引先の外圧、監督官庁の指導、あるいは内部事故があった

セキュリティ専門部署が存在する

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

第1章

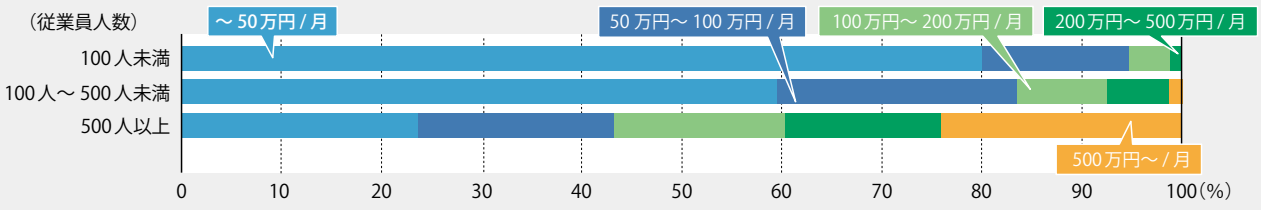
実情分析

セキュリティへの課題を感じつつも、予算が取れない実情。いかに効率よく対策を行うかが鍵となる

企業規模が大きいほど、セキュリティにかけるコストは大きいが、中堅企業の大半は月額50万円以下

セキュリティ対策においては、さまざまなコストがかかる。企業がどの程度のコストをセキュリティに割いているかという質問では、従業員100名以下の企業では、8割近い企業が月額にして50万円以下のコストだと回答している。一方で、100名以上の企業になると50万円以下という企業は減少する。しかし、従業員数100～500名未満の企業規模においても月額50万円以下の企業が6割程度と過半数を占めている。

従業員規模とセキュリティコストの内訳

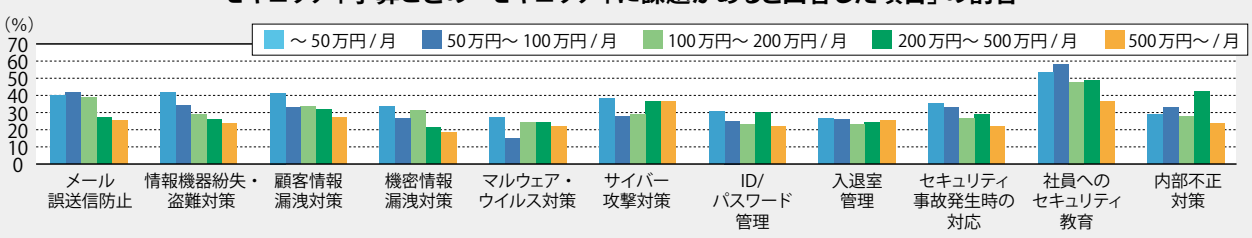


セキュリティコストを月額100万円以上かけている企業は、対策ができていると感じている割合が多くなる

下図にあるように、セキュリティコストを掛けたほうが、セキュリティに対する課題感が減少している傾向がある。おおむね、月額100万円を超えると課題を感じている割合が3割以下になってくる。次に、もう少し詳細に『どのようなセキュリティ対策が不足しているか』とコストの関係を見てみたい。メールの誤送信や情報機器の盗難・紛失といったヒューマンエラーのリスクは、コストをかけると減少していることがわかる。他の項目も多くはコストをかけると課題意識が減少しており、投資による『仕組み化』が進むことで効果が出ることが読み取れる。

一方で、グラフからは読み取りにくいが、予算をあまりかけていなくても、セキュリティに力を入れている企業は少なくない。むしろ『予算額がわからない』という回答の場合、セキュリティ対策が進んでいない傾向がある。まずは、自社のセキュリティ対策の状況を把握することが課題解決の第一歩と言える。

セキュリティ予算ごとの「セキュリティに課題があると回答した項目」の割合



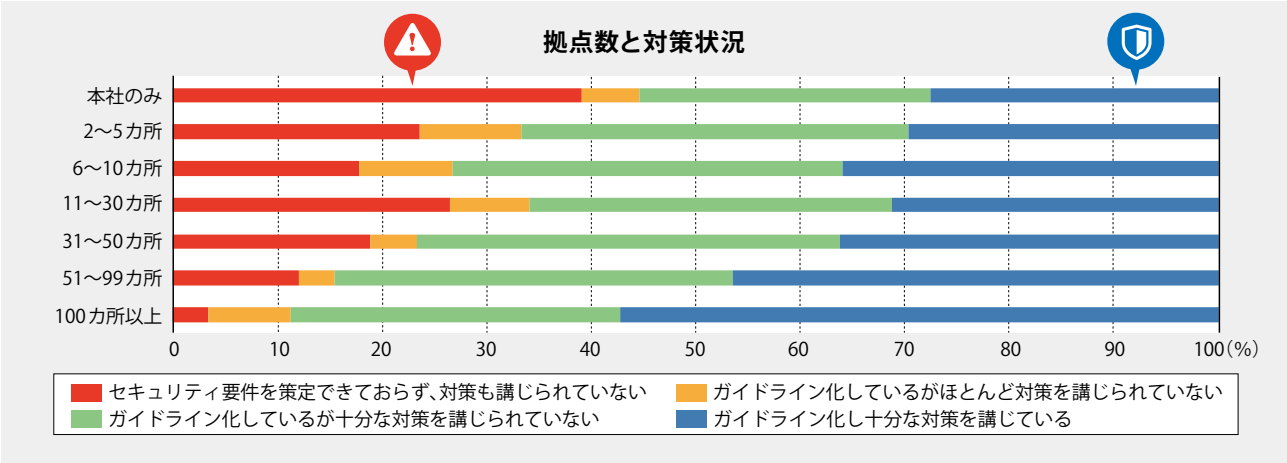
POINT!

コストを掛けるほど、セキュリティへの課題は減少する。
一方で、コストを掛けずに工夫して成果を出している企業も存在する

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

一般的に拠点数が増えるとセキュリティ対策は進む しかし、拠点数が増えることで セキュリティ対策が行き届かないケースが増える

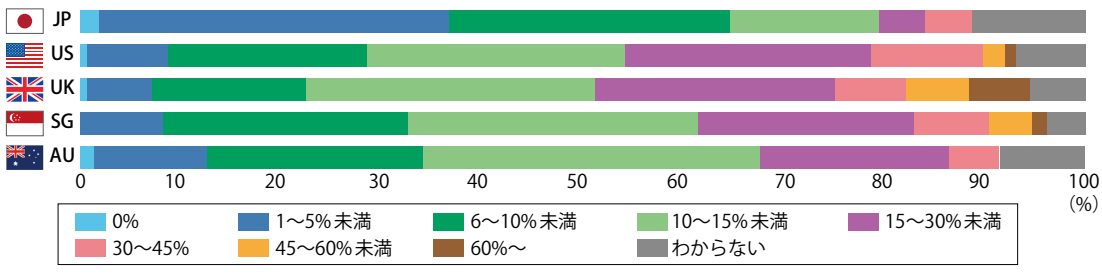
企業規模を測る一つの指標となるのが、拠点数だ。小売業や飲食業をはじめ、多くの拠点を展開する企業の場合、その拠点数とセキュリティ対策の状況には相関関係が見える。まず、本社だけの企業と拠点数が複数ある企業は、明らかに複数の拠点を持つ企業の方が、セキュリティ対策が進む傾向にある。興味深いのは、拠点数が11カ所を超えると、対策ができていない企業が増加している点だ。本社だけの場合はセキュリティへの危機感が薄く、拠点数が増えると意識が高まる一方で、一定の拠点数を超えると、各拠点まで目が行き届かなくなるという実態が想定できる。さらに拠点数が増えると状況が改善されることから、特に11～30拠点程度の規模が危険な規模だと言えそうだ。



Column

アメリカ・イギリス・シンガポール・オーストラリアのセキュリティ事情
企業のIT予算のうち、セキュリティが占める割合は？

日本企業では、月額でのセキュリティ予算は50万円以下が多数派だ。一方、世界ではどうだろうか。NRIセキュアの調査による『IT予算のなかで、セキュリティコストが占める割合』を見ると、日本の特殊な状況が見て取れる。アメリカ・イギリス・シンガポール・オーストラリアの4カ国の企業においてセキュリティコストがIT予算の中で10%以上となっている企業は、5割以上に及ぶ。一方、日本企業では、10%未満の企業が6割以上になっている。



※NRIセキュアテクノロジーズ「NRI Secure Insight 2018」より

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

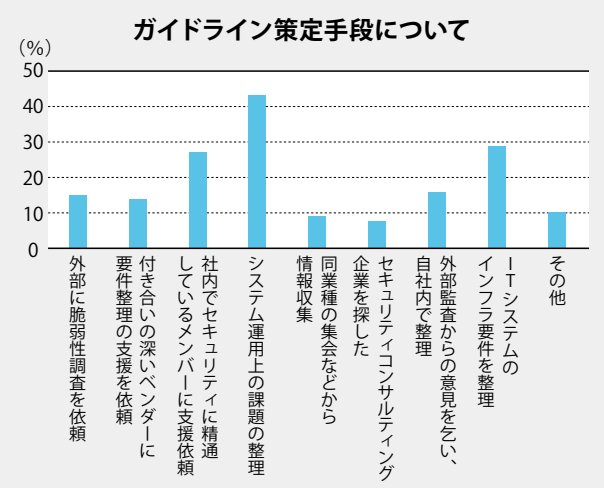
第2章

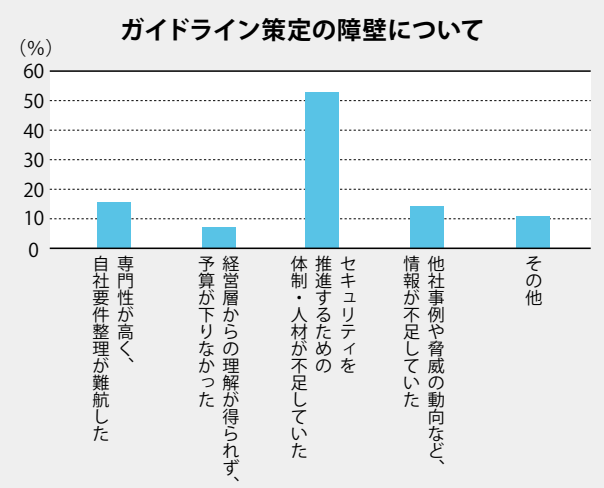
原 因

セキュリティ対策が進まない要因は、人・情報・コスト

ガイドライン策定に外部の力を借りない一方で、自社内での専門性の低さ、情報不足が課題となっている

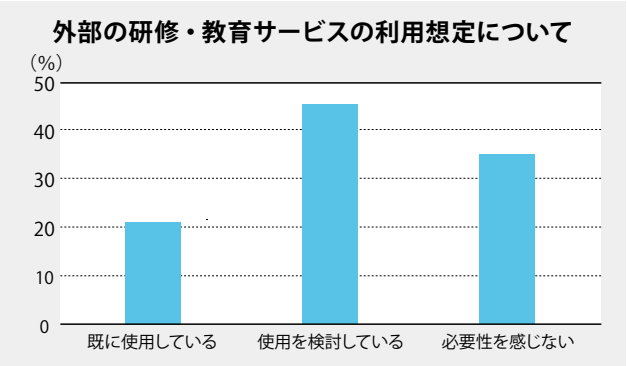
企業は、十分なセキュリティ対策が取れていない要因をどのように認識しているだろうか。本アンケートにおいて『セキュリティガイドライン策定にあたって、どのような手段をとったか』という設問では、『（自社内での）システム運用上の課題の整理』が43.6%、『自社内のセキュリティに精通したメンバーで行った』が26.9%など、『社内で行った』と回答する企業が多い。ところが、ガイドライン策定時の障壁としては『セキュリティを推進するための体制、人材が不足していた』という回答が半数を超える。自社内で十分な人材・情報がないと答える一方で、専門性が高い外部の支援を頼まないという矛盾した傾向が見える。





社員研修は「必要と感じつつ、実施されない」という矛盾

具体的なセキュリティ対策の実施状況を見てみよう。前項で、セキュリティ対策を進めるための体制や人材不足が明らかになっているが、セキュリティ担当者のスキルアップのための研修については、実施している企業は20.9%しかない。必要がないと回答した企業も34.5%も存在する。



POINT!

「人・情報・コスト」の不足を補う工夫が必要。
まずは「人・情報」を克服すれば、セキュリティ対策は進む可能性が高い

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

Column

コメントから見える担当者の本音

社員の
知識不足・職場風土から
積極的な問題対応ができない。

個人の
モラルや**リテラシー不足**

上長含めセキュリティに対する
認識が甘く対応が後手になりがち

今回のアンケートでは、各項目でさまざまなフリーコメントを記入してもらった。その中には『セキュリティ対策がうまく進まないことへの嘆き』ともとれるコメントが多い。人手不足、知識不足でありながら、社内での理解が得られず、対策が進まないことを憂えている声も多い。『個人のモラル・リテラシーの問題』『上長、経営陣の認識（理解）不足』『職場環境のせいで対応できない』といった、セキュリティの現実、上司の無理解、社内の環境の板挟みになっている情報システム担当者、セキュリティ担当者の悩みが切実に伝わってくる。

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

第3章

きっかけ

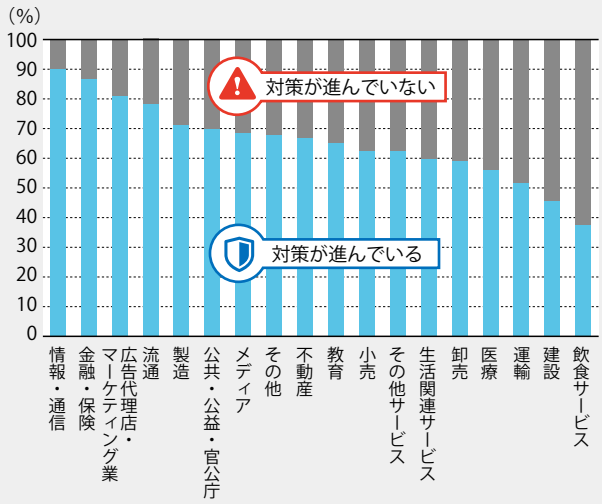
セキュリティ対策が行われるきっかけは『受け身』が圧倒的に多い

監督官庁からの規制が厳しい業界では、セキュリティ対策が進んでいる

セキュリティ対策が進んでいるかどうかを聞いた設問で、業種別に比較してみると興味深い結果が出た。情報通信業、金融・保険業、広告代理店・マーケティング業は、8割以上の企業が『セキュリティ対策が進んでいる』と回答している。一方で、運輸・建設・飲食サービス業などは、5割程度からそれ以下しか対策が進んでいない。

情報通信業、金融・保険業では顧客のデータを大量に扱うため、取引先からのセキュリティ要件への要求が高いこと、そのため監督官庁による管理があることが想定できる。広告代理店・マーケティング業では、多くの顧客から取引条件として高いセキュリティ要件を求められていると思われる。言い換えれば、監督官庁・顧客の要望といった『外圧』がなければ、なかなかセキュリティ対策が進んでいないと言える。

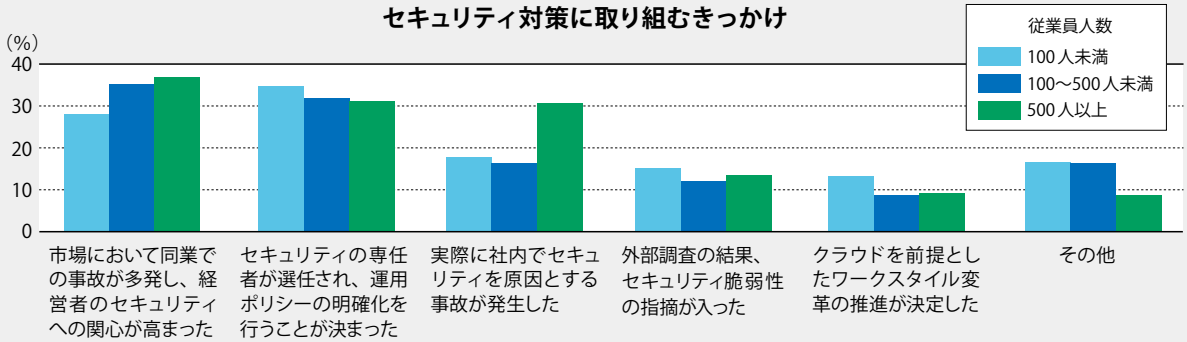
業種ごとの対策が進んでいる企業の割合



経営者がセキュリティに関心を持つと、対策が進み始める

セキュリティ対策を進めるきっかけとしては、『同業での事故が多発し、経営者の関心が高まった』というものが最も多い。続いて『セキュリティ専任者が選任され、取り組みが決まった』という回答が続くが、セキュリティ選任者の選定も経営者の関与が大きいと思われるため、『セキュリティ対策のきっかけ』の大半は、経営者の関心の高まりだと考えることができる。また、500名以上の規模になると、社内で具体的な事故が発生したことをきっかけとする企業が増える。

セキュリティ対策に取り組むきっかけ



POINT!

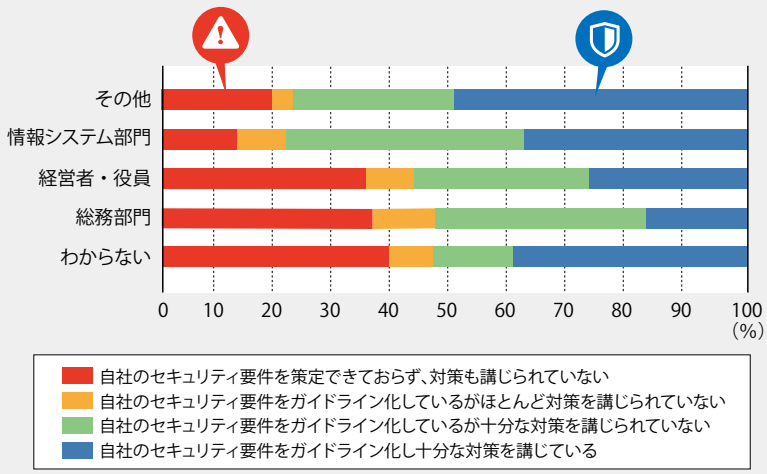
セキュリティ対策に取り組むきっかけは、“外部要因”と、“経営者の意識”に依存する部分が大きい

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

情報システム部門ではなく、セキュリティ専門部署の存在が鍵となる

今回のアンケートでは、それぞれの企業でセキュリティについて監督し、対策を進めていく部署としては、情報システム部門がそれを担っているという回答が半数を占めた。どの部門がセキュリティを担っているかと対策の状況を重ね合わせてみたところ、情報システム部門が担っている企業では、4割弱の企業が『対策が進んでいる』と回答しながらも、ほぼ同割合の企業が『対策が進んでいない』と回答している。実は『その他』と回答した企業が最も『対策が進んでいる』という結果になった。この『その他』は全体の5%程度だが、アンケートの自由記入欄でのコメントを見ると『その他』の実情は、コンプライアンス委員会やセキュリティ専門部署となっている。セキュリティ対策を進めるには、専門部署の設置が必須だと言えそうだ。

セキュリティ対策を推進する部門と対策状況の関係



POINT!

経営層の積極的な推進と専門部署によるオペレーションの両輪が鍵になる

Column

アメリカ・イギリス・シンガポール・オーストラリアのセキュリティ事情

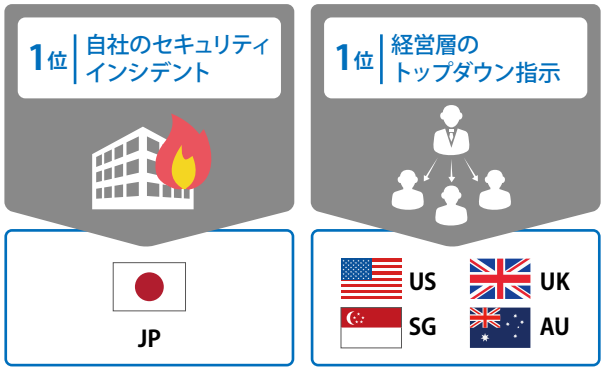
セキュリティ対策のきっかけの大半は『経営層の指示』

NRIセキュアの調査によれば、セキュリティ対策のきっかけとして、欧米では圧倒的に『経営層によるトップダウンの指示』だという結果が出ている。一方、同調査では日本企業（この調査では対象となったのは、ほとんどが従業員数1000人以上で7割が上場企業）では、自社内でのセキュリティインシデント発生をきっかけとしており、本調査と同じく『企業規模が大きくなると、なにかが起こってからの対応』と同じ傾向を示した。日本企業の場合、トップダウンで物事が進みにくいようだ。

中小・中堅企業では、比較的、経営層のトップダウンの指示が社内に浸透しやすいはずだ。なにかが起こる前にトップダウンでセキュリティ対策を進めることが重要だと言えるだろう。

情報セキュリティ対策実施のきっかけや理由

（当てはまるもの最大3つ選択）



海外4カ国の1位は共通して『経営層のトップダウン指示』であった。日本の1位は『自社のセキュリティインシデント』であり、"インシデントが発生してから対応する"という企業の割合が高かった。

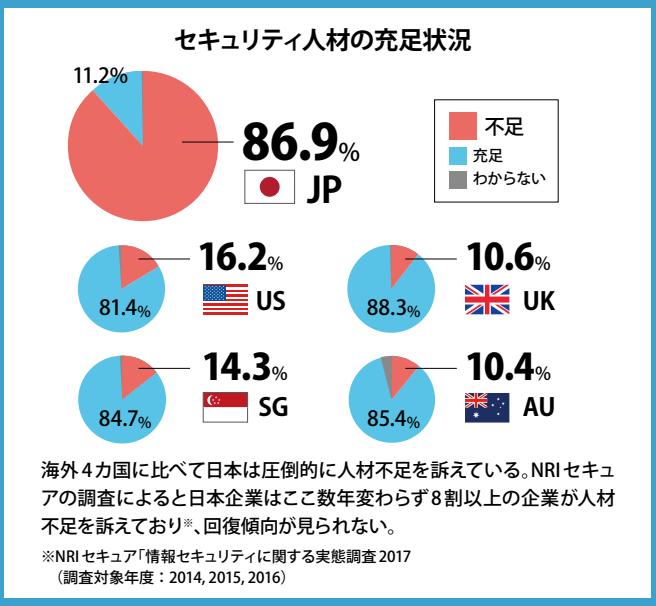
Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

Column

アメリカ・イギリス・シンガポール・オーストラリアのセキュリティ事情

セキュリティにおいて人材不足で悩んでいるのは日本だけ？

NRIセキュアの調査では、日本企業のセキュリティ対策での問題が浮き彫りになるものが多い。その一つが、『セキュリティ人材の充足状況』だ。日本企業は86%もの企業が『セキュリティ人材が不足している』と考えているが、欧米では、いずれも2割を下回る。イギリスやオーストラリアでは1割前後しか『人材不足』で悩んでいないという結果になっている。その背景には、欧米諸国のセキュリティ対策への取り組み方にある。人材が充足していると答えた欧米企業に『充足している理由』を聞いたところ『セキュリティ業務が標準化され、役割分担が明確』『セキュリティ業務が自動化・省力化されている』という回答が上位を占める。人材不足を人員の補充で対応するのではなく、業務のあり方を見直すことで対応していることが見て取れる。



海外4カ国に比べて日本は圧倒的に人材不足を訴えている。NRIセキュアの調査によると日本企業はここ数年変わらず8割以上の企業が人材不足を訴えており※、回復傾向が見られない。

※NRIセキュア「情報セキュリティに関する実態調査2017（調査対象年度：2014, 2015, 2016）

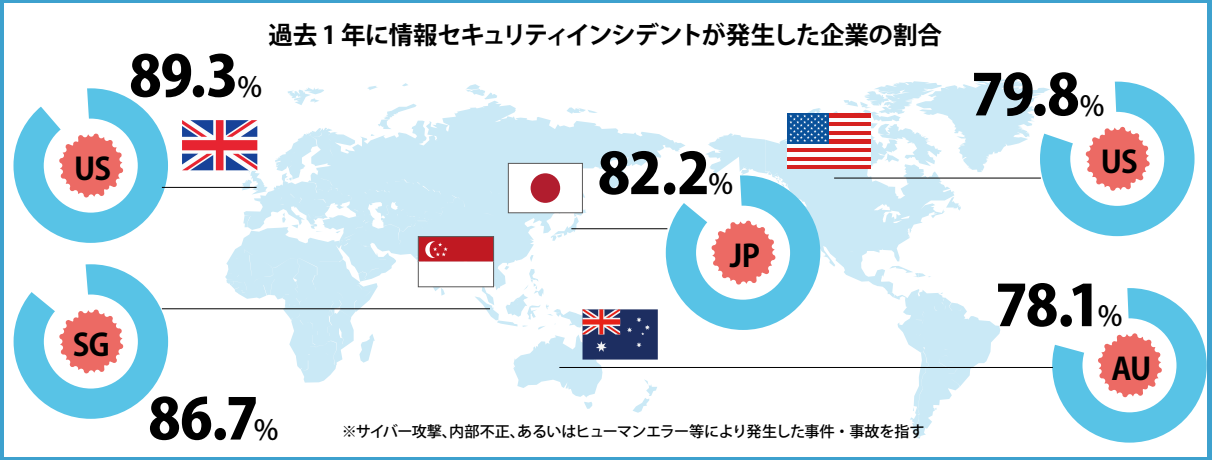
Column

アメリカ・イギリス・シンガポール・オーストラリアのセキュリティ事情

セキュリティ事故の発生は、世界で共通している

NRIセキュアの調査では、日本企業と欧米企業のセキュリティ対策の違いが目につく。調査手法・対象が異なるとは言え、本調査でもそれを裏付ける結果が出ている。

では、実際に世界ではセキュリティ事故はどの程度発生しているのか。下図を見れば分かるように、セキュリティインシデントは世界中で発生している。サイバー攻撃・内部不正・ヒューマンエラーなどによるインシデントは、調査対象である4カ国と日本では、同じように8割の企業で発生しているのだ。



Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

第4章
今後の取り組み

セキュリティ脅威から自社を守るために、なすべき4つのポイント

ここまで、アンケート結果の分析による『企業のセキュリティの実態』を解説してきた。その内容は、課題を感じつつも具体的な対策を十分に行えていない企業の姿が浮き彫りになった。

一方で、対策が進んでいる企業との違いも見えてきた。本資料の最後に、改めてその違いから見える『これからセキュリティ対策を進めるためのポイント』を4つ紹介しておきたい。

1 受け身ではなく主体的に取り組む

業種別にセキュリティ対策の状況を見た場合、情報・通信、金融・保険といった監督官庁のガバナンスが効いている業種では、対策が進んでいる事実があった。他にも、アンケート時のコメントで「取引先から取引条件としてセキュリティ状況の開示を求められた」といった回答もあり、親会社の監査など、外部からの指摘・要望によって、セキュリティ対策が進んだ場合が多い。

しかしながら、そういった外部からの圧力が少ない場合、セキュリティ対策を自社の問題と認識しにくいようだ。まずは外部の声ではなく、セキュリティ問題を自社の課題として捉え、主体的に取り組むことが大切だ。

2 経営層が意識を持ち担当者を明確にする

セキュリティ対策に取り組むきっかけで最も多かったのが、経営層の意識の高まりだった。海外でも経営層からのトップダウンでセキュリティへの対策が進む傾向がある。セキュリティ対策は、経営者が先頭に立って、コミットしていくことが欠かせないようだ。

そして、セキュリティ専門部署の設立は大きな要件だと言える。なにも専任の大げさな部署にこだわる必要はない。情報システム担当者だけではなく、部署を横断した「セキュリティ委員会」のようなものを立ち上げ、具体的な対策の立案、推進を行うのだ。誰がセキュリティ対策を推進するのかを明確化し、それを経営者が責任を持って支えていくことが、セキュリティ対策を浸透させていくだろう。

3 低予算でも取り組める対策を工夫する

残念ながら、現在日本企業の多くはセキュリティ対策に大きな予算を投じていない。全体として、セキュリティに投じる予算額が増えるほど、セキュリティ対策が進む傾向が見られたが、少額の予算でも対策が進んでいる企業も存在する。

まず考えるべきことは、自社のセキュリティ状況を把握し、何が不足していて、何をしなければならないかを洗い出すことだ。アンケートでも自社のセキュリティ予算を把握していない企業では、対策が進んでいなかった。自社の状況を知ることで、効率よく対策を進めることができるようになるだろう。

4 社内外の情報収集を徹底する

多くの企業は、人材不足・情報不足に悩んでいるが、セキュリティ対策そのものは自社内で解決しようとする傾向にある。情報がないと感じながら、専門家の力を借りることに抵抗があるという矛盾した結果だ。

そこでまず、外部からの情報収集に力を入れることと外部の専門家の意見を聞き、必要に応じて、専門性が高い業務をアウトソーシングすることを検討してもいいだろう。海外の企業では、人材不足を業務の標準化・自動化で解決している。情報収集によって、効率的な取り組みを実現しなければならない。

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

中小・中堅企業が効率よくセキュリティ対策を進めるステップ

まず、経営者が率先してセキュリティ対策を実行することを宣言し、
「セキュリティ担当者」を選任、社内に広報する。

1. 自社のセキュリティ状況を把握する

➔ まずは自社を知ること。社内のIT化の状況、スマートフォンなどの使用状況は
もちろん、「守るべき情報資産」とは何かを把握する。

2. 自社の最も危険性が高い分野を洗い出し、対策を考える

➔ STEP.1で把握した自社の状況に応じて、どのような脅威があるか、
それにどういった対応ができているかを洗い出す。

3. 社内研修などで、社内のセキュリティ意識を高める

➔ 制度・ルール・セキュリティサービスを導入するだけでは、セキュリティ対策は
進まない。社内のセキュリティへの意識が高まることは、大きな効果がある。

4. セキュリティ担当者を中心に社外研修などに参加、情報収集に務める

➔ セキュリティの分野は日進月歩で状況が変わる面がある。
外部の研修、専門家への情報収集を欠かさないことが大切だ。

Secure SketCH

30分でできるセキュリティ自己診断サービス
Secure SketCH

Secure SketCH（セキュアスケッチ）とは、NRIセキュアが提供するセキュリティ自己診断サービスです。設問に答えるだけで、900社以上のデータと比較をし、企業のセキュリティの「偏差値」や「対策の優先順位」などを確認することができます。
効率的にセキュリティ対策を実施するためには、現状のセキュリティレベルの「見える化」が欠かせません。ぜひお試しください！

>> **https://www.secure-sketch.com/**

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.

世界中の企業でセキュリティインシデントは頻発している。それは日本企業でも変わらない。

企業にとってセキュリティ対策への取り組みは必要不可欠なものだ。一度、情報漏えいなどの事故が発生すると、企業経営への影響は極めて大きなものになる。特に、中堅・中小企業では、場合によっては致命傷とさえなり得る。

だからこそ、適切なセキュリティ対策が必要だ。

本資料に目を通し、ぜひ、自社の状況と照らしあわせてほしい。そして適切なセキュリティ対策を実行し、健全な経営環境を整える一助となれば幸いである。

セキュリティ対策で効果的なソリューション

オフィス環境や社員向け情報セキュリティ教育サービスについては下記ページおよび、お問い合わせフォームよりお問い合わせください。

● KDDI まとめてオフィス　セキュリティ対策
>> https://www.kddimatomete.com/product/security/

お問い合わせ・お見積もり・お申し込み
https://bizpages.kddi.com/kmo_001.html

デバイス・ネットワーク・アプリケーション・インターネット接続などのセキュリティ対策については、下記ページをご確認ください。

● KDDI 法人のお客様向け　セキュリティ
>> http://www.kddi.com/business/security-managed/security/

お問い合わせ・お見積もり・お申し込み
https://bizpages.kddi.com/form01_504.html

※本資料に記載された情報は、2018年12月28日現在のものです。

KDDI まとめてオフィス株式会社　　**NRIセキュアテクノロジーズ株式会社**

Copyright © KDDI まとめてオフィス株式会社 , © NRIセキュアテクノロジーズ株式会社 , All Rights Reserved.