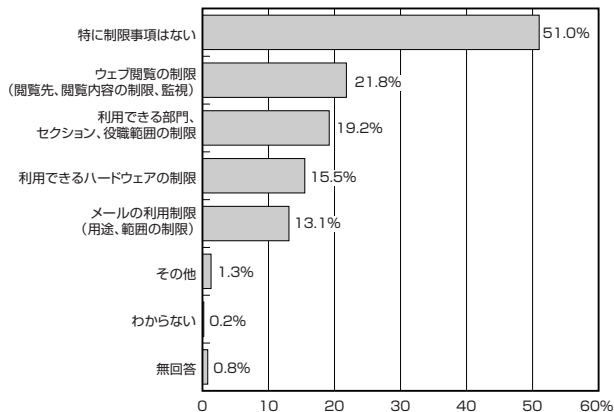


第4章 企業

利用制限・セキュリティー

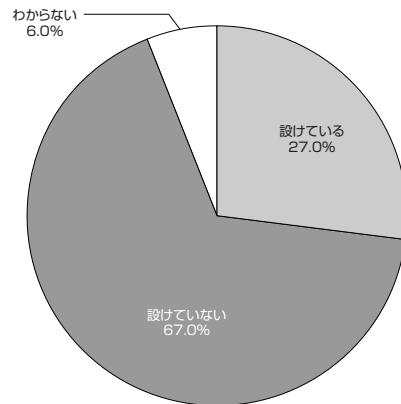
クラッキング経験企業は42.5%と急増

資料1-4-30 社内のインターネットの制限事項 N=1,662



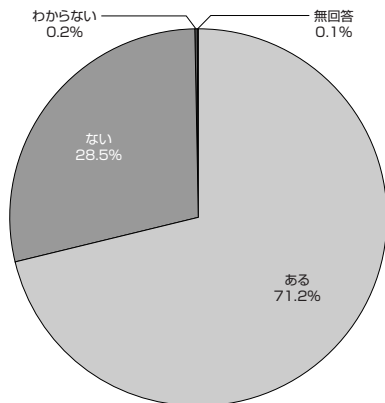
インターネット白書2001 ©インプレス, Access Media International,2001

資料1-4-31 社内クラッカー等への規制事項の有無 N=1,662



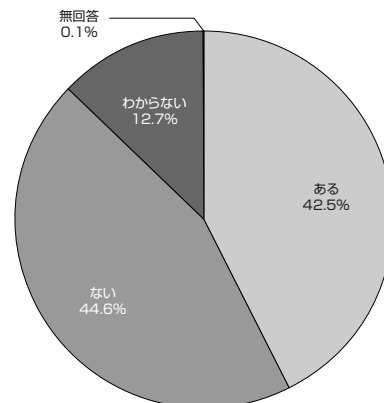
インターネット白書2001 ©インプレス, Access Media International,2001

資料1-4-32 ウイルス感染の有無 N=1,662



インターネット白書2001 ©インプレス, Access Media International,2001

資料1-4-33 クラッキングされた経験の有無 N=1,662



インターネット白書2001 ©インプレス, Access Media International,2001

解説

■ 利用制限・セキュリティー

インターネットの利用が進むにつれて、セキュリティーの問題は重要度を増している。従業員1人1人にインターネットのアカウントを発行することは、同時に社内外からの不正アクセスの機会を増やすことにも繋がるということを、企業がどのように受け止め、その対策を講じているかを、社内の利用制限の有無や外部からの不正アクセスという点から聞いている。

インターネット利用に関する社内の制限事項については昨年と比べてやや厳しくなっているものの、51.0%が「特に制限

事項はない」と回答している。ここでは基本的にはインターネット利用のメリットを損なわないという企業の姿勢がみられる。

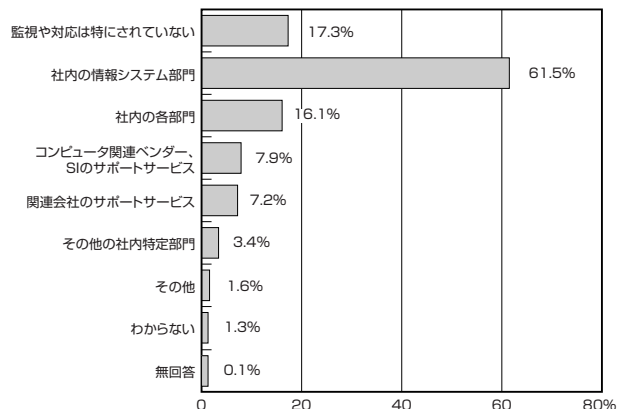
今年初めて掲載したデータは社内クラッカー等への規制事項の有無であるが、「設けていない」という回答が7割近くを占め、社内的な対策は遅れているといっていよう。何らかの規制事項を「設けている」比率が高いのは、従業員規模が500人以上の大規模企業で、5割以上が「設けている」と回答している。

また、最も多いと考えられる被害であ

る「ウイルス感染の有無」についても全体の7割以上が「ある」と回答している。従業員規模が多くなるに従い感染機会も増えるため、500人以上の従業員規模では9割近くに達することから早急な対策が望まれる状況であることは間違いない。

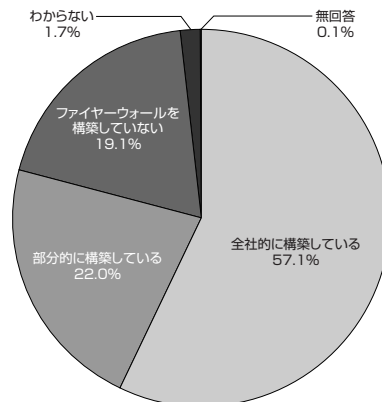
さらに実際にクラッキングされた経験も聞いている。「ある」と回答した企業は42.5%と1999年の5.7%、昨年の10.3%から急増している。ただし、回答企業の利用歴が長くなっていくとともに遭遇する率は当然ながら高くなり、全体に経験した率も増加していく。また、今年クラ

資料 1-4-34 社内クラッカーについての監視や対応 N=1,662



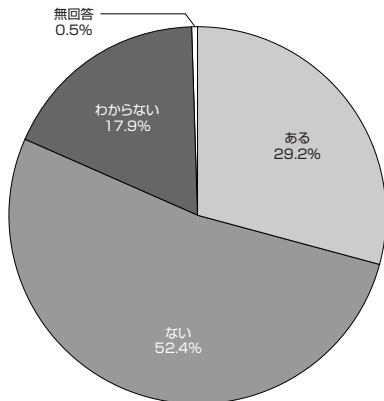
インターネット白書2001 ©インプレス, Access Media International,2001

資料 1-4-35 ファイアーウォールの構築有無 N=1,662



インターネット白書2001 ©インプレス, Access Media International,2001

資料 1-4-36 ファイアーウォール以外のセキュリティ対策の有無 N=1,662



インターネット白書2001 ©インプレス, Access Media International,2001

解説

ッキング経験の定義を「アタックの痕跡までを含み、実際の被害の有無は問わない」と明確にしたため、これを差し引いて考えなければならない。しかしながら、今後利用がさらに拡大するに従って、セキュリティ対策の重要性が増すことは間違いない。

社内クラッカー等への規制事項の有無と同様に、今年初めてその監視体制や対応についても聞いている。

「監視や対応は特にされていない」回答も17.3%みられるが、従業員規模別では0～9人規模で47.5%に上り、5000人以上

では0.0%と、規模によりその状況は大きく異なる。具体的な対応を行っているのはほとんどが「社内情報システム部門」で、そうした部門を持たない小規模企業では外部の「コンピュータ関連ベンダー、SIのサポートサービス」や「社内の各部門」に頼らざるを得ないという状況がうかがえる結果となっている。

ファイアーウォール構築に関しても、大規模企業のほうが全社的に構築している場合が多い。

ファイアーウォール以外のセキュリティ対策については全体の約3割が講じてい

ると回答しており、これも従業員規模別でみると大規模企業で多くなっている。

この状況から、大規模の企業と比較してシステム管理に多くの人員を割くことができない小規模の企業のほうが、よりセキュリティ対策を万全にする必要に迫られているといえる。

(矢野さよみ アクセスメディアインターナショナル株式会社)



[インターネット白書 ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<http://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp