

第13回 企業情報の守り方と対策について



Profile プロフィール

トレンドマイクロ株式会社 上級セキュリティエンジニア

染谷征良

ヨーロッパ、北米、日本のITセキュリティ業界で、競合分析、製品・技術戦略からマーケティング、営業、サポートなど、15年以上の実務経験を有する。

企業情報を守るために社員のセキュリティ意識変革を

社内情報を扱う社員のセキュリティ意識の低さが、サイバーリスクを引き起こしているケースは少なくありません。ひとたびセキュリティ犯罪の被害にあれば、企業が失うものは甚大です。社員一人ひとりに認識してもらえるよう、社内で取り扱う情報の重要性を、折に触れて伝えましょう。サイバー犯罪関連のニュースを定期的に社内メールで配信したり、朝礼で事例を紹介したりするだけでも注意喚起につながり、業務データの持ち出しなどの内部犯行の抑止力にもなります。

社内で業務データを扱う際の経験



■ 禁止されているツールで外部とデータを共有	54.8%
■ 自分の担当外のデータにアクセスした	13.8%
■ 持ち出し禁止データを外部に持ち出した	7.9%
■ 退職時にデータを持ち出した	4.4%

出典:2014年7月トレンドマイクロ実施
「企業における業務データ取扱い実態調査2014」

従業員のセキュリティ意識の向上の取り組みに加えて、以下のような具体的な対策もお勧めします。

■ 利用中のソフトウェアを最新に保つ

OSやソフトウェアの修正プログラムは、自動更新にして常に最新を保ちましょう。昨今急増している脆弱性を狙った攻撃からのリスクを大幅に軽減することができます。

■ パスワードは使いまわさない

パスワードは、できるだけ文字数を多く、かつ複数の文字種や大文字・小文字を混ぜて作りましょう。定期的にパスワードを変更すること、複数のサービスで同じパスワードを使いまわさないことも重要な対策です。

■ 総合セキュリティソフトの利用を

ウィルス対策ソフトより多機能な、総合セキュリティソフトの導入がおすすめです。また、全社的な管理が難しい場合は、中小企業向けのパッケージサービスを利用すると、社内のPCやスマートフォンのセキュリティ対策を一括して行えるほか、コストダウンや運用負荷を軽減することもできます。

以上を踏まえ、広い視野で、貴社にとって最もよいセキュリティ対策を検討してみてください。