セキュリティ対策虎の巻（第4回）

内部脅威対策は「アクセスログ」より始めよ

2016.09.28

セキュリティーに完全無欠の対策はない。企業を取り巻くさまざまなリスクに対応するには、脅威の種類を理解し、的確に対応しなければならない。社内システムへの不正アクセス・ウイルス感染・データ改ざん、メールやUSBメモリーを悪用した内部からの情報漏えい、自然災害によるデータの消失ーー。どんな脅威から情報を保護するかによって、対策も異なってくる。

「セキュリティー対策の必要性は理解しているが、どのような脅威から、どうやって、どのレベルまで防御すればいいのか分からない」。こんな悩みを持つ中堅・中小規模の企業経営者が多い。セキュリティー対策といえば、まず外部からの脅威を思い浮かべる。外部脅威への対策についてはこれまで述べてきたが（下記「関連記事」「連載記事」を参照）、悪意のある人がパソコンのUSBケーブルをハードディスクにつないでデータを改ざんしたり、盗んだりするリスクには対応できない。内部犯行による情報漏えいには、内部犯行用の対策が求められる。

内部犯行の抑止に役立つアクセスログ管理

内部犯行の多くのケースでは、犯行者は何らかの足跡をシステムに残す。「いつ」「誰が」「どのデータ」にアクセスしたのか、アクセスログ（履歴）を取得・保存しておけば、情報漏えいやデータ改ざんの問題発生時に、そのログを原因究明に役立てられる。

アクセスログ（以下、ログ）は建物の出入り口に設置された防犯カメラのようなものだ。トラブル発生時に録画映像で現場を確認するのと同様に、情報漏えいが疑われる問題発生時にそのデータを基に原因を究明する。

例えば、従業員が権限外のシステムにアクセスしたり、社内のパソコンからUSBメモリーにデータをコピーしたりした場合、ログ情報を基に関係者を特定できる可能性がある。ログで証拠を示すことにより、取引先や関係者に状況を説明したり、ログの取得を社員に通知して、内部犯行による情報漏えいを抑止したりするといった効果も期待できる。

ログ管理と一口に言っても、ネットワークやサーバー、アプリケーションなど対象は幅広い。ログをやみくもに集めていても管理しきれなければ意味はない。そこで、重要情報を保管するファイルサーバーのログ管理に的を絞り、不正アクセスや情報漏えいの抑止と検証に役立てるといった工夫が欠かせない。最低限、重要情報を保管するファイルサーバーのログは取得できる仕組みを構築すべきだ。

世の中にはさまざまなログ管理製品が提供されている。ログの取得・保存に加え、ログを監視して異常時にシステム担当者に通知したり、ログの解析結果をレポートしたりする機能を備えるタイプもある。何を目的とするかで選択の基準もさまざまだが、せっかく内部犯行対策を行うなら、データ消失にも備えられるソリューションがいいだろう。

ログ管理が可能なサーバーで安全にデータを保管… 続きを読む