# オペレーティングシステムのログ

## ３種類の管理すべきログ

セキュリティツールのログ
オペレーティングシステム（ＯＳ）のログ
アプリケーションのログ


システムイベント
監査記録

| | |
|---|---|
| Unix、Linux 系 | syslog |
| Windows 系 | イベントログ |

IT セキュリティのための管理すべきログには、大きく分けて、セキュリティツール、オペレーティングシステム（OS)、アプリケーションの 3 つの分野でのログがあります。
その中で、サーバや PC、ネットワーク機器などの OS から出力される情報には、セキュリティ対策にとって有用な情報がたくさんあります。
OS からのログは、一般的には、サービスの開始などの OS 内部で実行される動作として出力される「システムイベント」と、認証やアクセス権限に基づくセキュリティイベントの情報をしての「監査記録」があります。
「システムイベント」では、タイムスタンプや、イベントコード、ステータスコード、エラーコード、サービス名などの情報が記録されます。「監査記録」は、認証の成功や失敗、セキュリティポリシーの変化、ファイルアクセスなどの権限の行使など監査の対象となるようなセキュリティイベントの情報が記録されます。いづれのイベントについても、主だった種類の OS で、管理者が出力すべきログを指定できるようになっています。
OS から出される様々な情報のログの多くは、syslog 形式で出力されます。
メインフレームを知っている方には、SYSLOG というと JES2 などのジョブ入力サブシステム で提供する SYSOUT データセットのことですが、通常 syslog は、UNIX や Linux でデファクトスタンダードになったクライアント･サーバ型の IP ネットワーク上で転送するための標準規格である通信プロトコルのことを指します。
ログを収集するには、最適なフォーマットだということで、様々な機器やシステムで採用されています。
ルータなどの syslog 送信側から、syslog メッセージは、UDP または、TCP の 514 番のポートを使用して、1k バイト以下の短いテキストメッセージで syslog サーバなどの受信側に送信します。Linux では、syslog デーモンが、メッセージを記録し、通常セキュリティの関係上ログは root 権限でないと読み込めないようになっています。
Windows 環境では、イベントログと呼ばれ、バイナリのファイル形式で、syslog の logger コマンドに対して、eventcreate コマンドでログを記録することが可能です。
OS のログは、セキュリティインシデントが発生した場合の、分析や対処のために非常に大切な情報となるため、ログ管理としては、基本的に必須で管理すべき重要なログです。


© CEC Customer Service Ltd.