4A-5

情報セキュリティサービス（2）
ーデジタルトレーサビリティー

鶴川 達也†、安田 晃久†、北上 眞二†
三菱電機株式会社

1. はじめに

今日、企業情報システムにおいて、情報漏洩などセキュリティ問題発生時の原因解析や、システムが正しく運用されていることを客観的に示すことなどを目的に、ログの収集保存が行われている。

しかし、ログの形式や内容、記録されている ID の意味などがアプリケーションやシステムごとに異なっているため、収集保存は行われているものの、上記目的のための利活用が十分に行われているとは言い難い。

この様な背景の下、多数のログからユーザの行為や操作の追跡を容易に可能とし、セキュリティ向上を目的としたログの利活用を高める、デジタルトレーサビリティシステムを開発した。

2. 原因解析におけるログ利活用の課題

ログを収集保存しても、一般的にアプリケーションやシステムごとにログファイルが異なる、記録されているユーザや機器の ID が各ログ固有のものであるといった問題を抱えている。また、解析性向上に役立つ、ユーザや機器の属性情報（所属名、設置場所など）は、ログに含まれていない場合が多い。

従って、セキュリティ問題が発生した時、ログの解析により原因を追究する上で、以下に挙げる課題が存在する。

(1) 複数ログの統合解析が困難

ユーザの行為、操作の履歴が、複数のログに跨って記録されており、ユーザ操作の全貌を把握することが難しい。

また、ユーザ ID や機器 ID が各ログ固有の ID で記録されており、異なるログ同士を結び付けて解析することが難しい。

(2) ログに記録されている ID が実体と結びつかない

ログからユーザ・機器などの ID が分かっても、実体（具体的な人や機器）と結びつかず解析が進まない。また、解析対象のログが古いと、この問題がより顕在化する。

(3) ユーザや機器の属性情報を解析に利用できない

ユーザや機器の ID をログに記録しても、それに付随する属性情報（ユーザであれば所属、役職など、機器であれば機器種別や設置場所など）まではログに記録されない場合が多い。属性情報は時間とともに変化することもあり、ログとこれらの情報と組み合わせることによる解析性の向上を図ることが難しい。

3. デジタルトレーサビリティシステム

本節では、デジタルトレーサビリティシステムの構成について説明し、2 節で挙げた課題をどのように解決しているかについて述べる。

今回開発したシステムの構成を図 1 に示す。

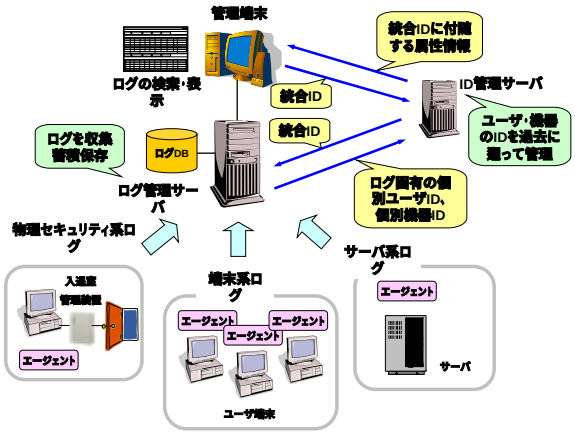

図 1 システム構成

デジタルトレーサビリティシステムは、端末やサーバ、物理セキュリティ装置などに導入したエージェントによりログを収集し、ログ管理サーバ上でフォーマットを統一し一本化してログ DB に蓄積保存する、ログ統合管理システム[1]をベースとしている。

さらに、ユーザ・機器の ID 及び付随する属性情報を過

Information Security Service (2) - Digital Traceability -
† Tatsuya Tsurukawa, Akihisa Yasuda, Shinji Kitagami : Mitsubishi Electric Corp.

去に遡って管理する ID 管理サーバ、ログ管理サーバに蓄積保存されたログを検索・表示する管理端末から構成されている。

3.1 ID 管理サーバによる統合 ID の照会とログへの反映

ログ管理サーバでは、エージェントから送られてくるログをログ DB に蓄積する前に、ログに含まれるログ固有のユーザ ID、機器 ID から、ID 管理サーバと連携して統合 ID を照会し、ログに反映してから蓄積する。

ここで、ログ固有のユーザ ID は例えば端末のログオンアカウントやメールアドレスなどが該当し、機器 ID は例えば端末のマシン名や IP アドレスなどが該当する。

一方、ID 管理サーバが管理する統合 ID は、人事情報や資産管理情報といった、ユーザ、機器の実体に直接結びついた情報に割り付けられた ID である。

以上のようなログの加工をログ蓄積時に全てのログに対して施すことにより、複数ログに各ログ固有の ID で記録されたユーザや機器の ID を統合 ID で紐付けることができ、異なるログ同士を結び付けてユーザ操作の全貌を把握することが可能となる。

これにより、2 節(1)で述べた、複数ログの統合解析が困難となる課題を解決している。

3.2. ログの検索・表示

ログ管理サーバに蓄積保存したログを、検索・表示する管理端末の画面を図 2 に示す。

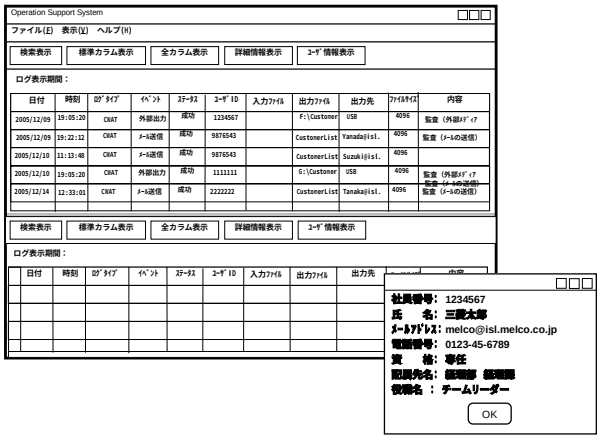

図 2 ログの検索・表示画面

ユーザ名、機器名、ファイル名など各種データをキーとした検索結果を時系列で表示することができる。さらにログ蓄積時にログに反映した統合 ID も検索キーとすることができるため、例えば入室し、端末にログオンし、ファイルにアクセスし、印刷し、退室するといった、特定のユーザの全ての操作を時系列に表示することができる。

また、管理端末もログ管理サーバ同様、ID 管理サーバと連携し、統合 ID を元にそれに対応する人事情報や資産管理情報を引き出して表示することで、逐次実体情報を参照しながらログを解析することができる。

解析対象ログが古く、該当ユーザが退職しているような場合でも、レコードの日付時刻から、在籍当事の過去の人事情報を引き出して表示することにより、過去に遡ったログの解析性を確保することができる。

これにより、2 節(2)で述べた、ログ中の ID が実体情報と結びつかず解析が進まなくなる課題を解決している。

3.3 属性情報を利用した解析

管理端末でログを検索・表示した後に、ID 管理サーバと連携し、統合 ID に付随する一部の属性情報を照会、追加表示することができる。これら属性情報をログ蓄積時に反映してしまうとログサイズが不必要に増大し、ログ DB の容量が無駄に使われてしまうが、検索して絞り込んだ後にログに反映することでこの問題を解決しつつ、ログ解析時の属性情報の利用を効率的に行うことができる。

例えば情報漏洩が発生し、該当ファイル名が判明しているものの、それがどの部署で管理されているものか分からないような場合、ファイル名でログを検索・表示した後、部署名を追加表示する。その後、部署名でソート、集計を行い、そのファイルに最も多くアクセスしている部署がそのファイルの所有部署であると推定することができ、ログの解析を向上させることができる。

これにより、2 節(3)で述べた、ユーザや機器の属性情報を解析に利用できない課題を効率よく解決している。

4. おわりに

以上のように、収集ログの蓄積時にログに適切な加工を施し、後の解析性を高めることで、企業情報システムのセキュリティ管理におけるログの利活用を向上させる、デジタルトレーサビリティシステムを開発した。

今後は、このシステムを実際に活用、有効性を評価し、さらなるログの利活用向上を進めていく。

参考文献

[1] 樋口他,“ 情報漏洩防止ソリューション（４）－ログ収集管理－ ”,情報処理学会第 67 回全国大会,3A-7,2005