熊本中央信用金庫

熊本中央信用金庫

シンクライアント環境でのログ分析を可能にしたLogStare

熊本中央信用金庫は熊本県全域をサポートする九州中堅の金融機関である。大正12年に創設され、長年にわたり地域経済の活性化に努めてきた。同金庫では以前からログを重要視しクライアントPCのログ保存を行っていたが、ITシステムを本部のサーバ・ベース・コンピューティングによる一元管理体制に強化したところ支障が出た。その問題を解決するべく導入したのがセキュアヴェイルの「LogStare」だった。同金庫でIT管理を担当する事務集中部 部長の原口啓二氏、代理の佐伯義朝氏に話を伺った。

熊本中央信用金庫では個人情報保護法施行の前に、あるログ管理ツールを導入した。ログを保存することは、情報漏えいなどの問題が起こったときに流出元を調査するのに役立つ。個人情報を保護するには必要な対策であった。

その後同金庫では、さらにセキュリティを強化するために Citrix 社の MetaFrame（現在の名称は Citrix XenApp）を導入した。これはシンクライアントの一種で、ユーザの使用環境をサーバで一元的に管理するものだ。ユーザはクライアント PC を操作しながらも、実際はサーバ上のアプリケーションやデータを使用することになる。メンテナンスも軽減されるなど導入メリットは大きい。ところがログ保存という面で新たな問題が立ち上がった。

事務集中部長の原口啓二氏は「以前はクライアント PC の中に個人情報を含むデータが保存されていましたが、MetaFrame 導入によって外部流出させてはならないデータはすべて本部のサーバで一元的に管理するようにしました。しかし、それまで使用していたログ管理ツールでは MetaFrame を使用したアクセスログの一部が取れなくなってしまったのです」と当時の状況を語った。

従来から使っていたログ管理ツールは、クライアント PC のログを保存するタイプだった。MetaFrame はサーバ上のアプリケーション、データを扱うシステムなので、一部の操作が記録されなかったのだ。その対策を検討していた原口氏が相談を持ちかけたのは、同金庫の IT システムのコンサルティングや構築、保守などを請け負っている株式会社オリテック九州の宮川起典氏だった。宮川氏に紹介されたのがセキュアヴェイルの統合ログ管理システム LogStare である。サーバへのアクセスログを保存する LogStare なら MetaFrame を使ったアクセスログをすべて保存・分析することができた。

LogStare を紹介した理由を宮川氏は「サーバのログをとるのは容易ではありません。CPU に大きな負荷か掛かればアプリケーションのレスポンス速度に影響を与えます。またツールの相性が悪い場合にはアプリケーションがロックしてしまうケースも考えられました。いろいろ調査してみて最適と思われたのが、サーバへの負荷とアプリケーションへの影響が少ない LogStare でした」と語った。

宮川氏は、持ち込んだノート PC を使って LogStare のデモを行い、それを目にした原口氏はすぐに導入を決定した。平成 18 年（2006 年）のことである。

見つけた不審なログからアクセス元を効率的に探していける LogStare

同金庫が LogStare で監視し分析しているのはファイルサーバへのアクセスだ。ファイルサーバには個人情報を含むデータベースは保管していないのだが、職員が日常的に作成する文書には個人情報が含まれる場合もある。そういうデータへのアクセスログを LogStare で監視しているのだ。同金庫に導入された LogStare は、ネットワーク内のファイルサーバと MetaFrame の間に設置され、その間を流れるデータを読み取って記録する。

熊本中央信用金庫 事務集中部長
常勤理事
原口 啓二 氏

熊本中央信用金庫 事務集中部
事務集中課 代理
佐伯 義朝 氏

NTTデータ ジェトロニクス株式会社
ビジネスパートナー
株式会社オリテック九州
システム営業部 部長
宮川 起典 氏

熊本中央信用金庫

金庫概要

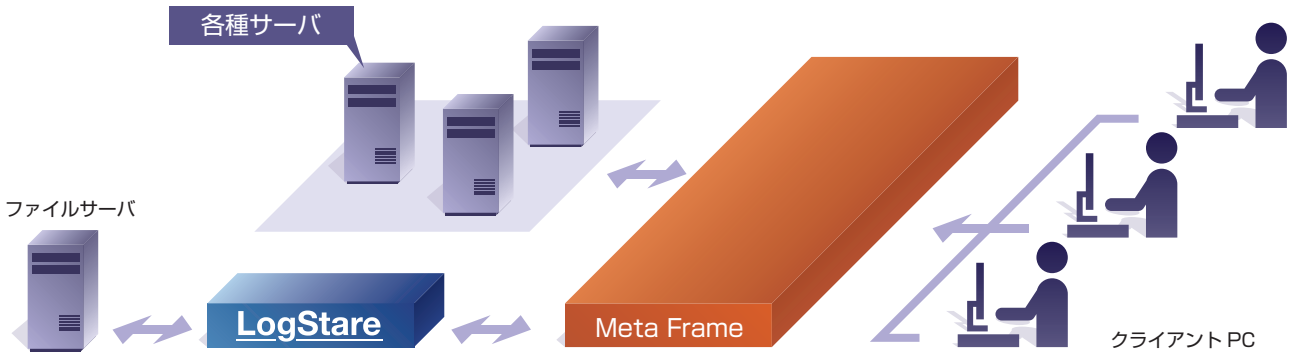
事業内容：信用金庫法に基づく金融業務

大正12年の創立以来、"良い家庭、良い企業、良い社会の育成発展のために、金庫の総力を結集し金融の円滑をはかる。"という基本方針を掲げ、地域に密着した営業を行ってきた。地域密着型金融の担い手として、地域経済の活性化や中小企業金融の円滑化のための機能強化に向けた取組みを推進している。

URL：http://www.kumachu.jp/

熊本中央信用金庫

熊本中央信用金庫　システムイメージ



ファイルサーバは日常的に職員全員が利用するものなので、特殊な動きがあればグラフですぐにチェックできる。LogStareの運用を始めて約３年。例えば一度に大量のファイルへのアクセスがあり、それがコピーされていたケースでは、ユーザが持ち出したのではなく、サーバ内の別の場所に保存し直しただけだった。これはそれまでのログ管理ツールであれば、単にコピーを行ったというログであるが、LogStare導入により、そのファイル数がグラフ化されているため、「通常ではない動き」に着目し調査することが容易になったという。（なお、当然ながら、同金庫ではUSBメモリ等への書き出しはシステムにより制御されている）

事務集中部 代理の佐伯氏はLogStareについて次のような感想を持っている。

「ログが見やすかったというのが最初の印象です。まずログを単なる文字の羅列ではなく、グラフなどで視覚的に見られます。それからLogStareは監視したいファイルやフォルダを起点にしてログを調べられます。重要なファイルを見た人が誰なのか、いつアクセスしたのかを調べて、不審な点があればそこから詳しくドリルダウンしながら見ていくことができます」

以前のログ管理ツールはクライアントPCでの操作ログを保存するものであったために、調査をするときは「どのパソコンから操作したのか」を先に見当をつけておく必要があった。それに対してLogStareでは、サーバへのアクセス状況を見て不審があればそこからドリルダウンして、いつどのパソコンから誰がアクセスしたのかを調査していく。営業店（支店）では１台のパソコンを複数の職員で使う場合もあるので、そのような環境でアクセスしたユーザを特定するのにMetaFrameとLogStareの組み合わせは向いていた。

LogStareのもうひとつの長所として佐伯氏は「大きなスパンでログを見られること」を挙げた。仮に一日単位という短いスパンでの分析に限定されているのなら、その日のチェックを忘れてしまえば問題を見逃してしまう可能性がある。LogStareは月単位、週単位でのまとまりでグラフ化して分析できるので、異常なログを見つけた場合はそこから「どの日のアクセスが異常なのか」を探すことが可能だ。

LogStareがあるからこそ、シンクライアント環境が安心して使用できる

現在同金庫では月一度の間隔で定期的なチェックを行っているが、作業に費やす時間は２～３時間と負担は軽い。しかし佐伯氏はそれだけではなく、「日頃からLogStareの画面を見て、不審なことがないか、きちんとログが取れているかをチェックするよう心がけている」という。「異常があればすぐに気が付くし、ログが取れていなければ定期的なチェックができないから」というのがその理由だ。それでも作業にかかる時間は一度に５分程度にすぎない。

原口氏は「お客様の個人情報を守るのは金融機関の使命。金庫の姿勢に対するお客様の目も厳しい。LogStareを導入したことで、セキュリティの高いMetaFrameのシステムが安心して使用でき、仮に情報漏えいなどの問題が起こったとしても原因や流出元を追求できるようになった」と導入したメリットを語った。

SecuAvail
株式会社セキュアヴェイル
本社：
〒530-0044　大阪府大阪市北区東天満 1-1-19 アーバンエース東天満ビル
TEL：06-6136-0020
E-Mail：sales@secuavail.com
URL：http://www.secuavail.com