

すべてのパソコン操作のトラッキングに加え、抑止効果によりシステムのセキュリティレベルを飛躍的に向上



CWAT導入効果

- すべてのパソコン操作のトラッキングにより不正処理の追跡が可能に
- すでに施行していたセキュリティポリシーを、システム導入でより確実に
- 操作の瞬間にアラートを表示することで不正操作の抑止効果を発揮
- 利用者から管理者に至る複数レベルでのセキュリティ管理を実現

お客様プロフィール

※平成18年3月31日現在

- 名称: 城北信用金庫
- 創立: 大正10年5月31日
- 本部: 東京都北区豊島1-11-1
- 店舗: 115店舗(内30有人出張所)
- 預金量: 2兆2,879億円
- 職員数: 約2,200人

「地域住民の幸福」「地域企業の繁栄」「地域社会の発展」への貢献を経営理念として掲げ、地域に密着した質の高い金融サービスを提供する城北信用金庫。取り扱い情報の保護を重要視する同信金では、個人情報保護法の施行を機にセキュリティ対策及び関連システムの刷新を計画。複数のプロジェクトを推進してきました。資産管理、個人認証システム等を導入後、長年の懸案対象であった内部情報漏洩対策の一環である「パソコン操作監視・抑止及び操作履歴の取得システム」のプラットフォームとして同信金が選択したのは、情報セキュリティマネジメントプラットフォームCWAT(シーワット)でした。

導入の経緯:個人情報保護法の施行を機に、さらなるセキュリティ強化を目指す

「金融機関として以前から重点をおいてきたセキュリティ対策ですが、個人情報保護法の施行を機に、そのさらなる強化を図るため、関連システムの刷新を計画しました」今回の情報漏洩対策システム導入に至った経緯について、城北信用金庫(以下、城北信金)システム部システム企画グループ 次長の濱田良直氏はこう語ります。

2004年1月、王子、日興、太陽、荒川の4信用金庫が合併し誕生した城北信金では、合併に伴うシステム対応が一段落した後、個人情報保護法への対応を念頭に、全社システムのセキュリティ強化に向けたプロジェクトを開始。資産管理、個人認証システムなどの導入完了後、長年懸案となっていた内部情報漏洩対策システムの一環である「パソコン操作監視・抑止及び操作履歴の取得システム」の構築に向け、プラットフォームとなるソフトウェアの選定作業を開始しました。

選定のポイント:ログトレース、禁止、抑止効果の全てを網羅した唯一の製品として

日頃の業務処理においても、セキュリティに気を配った運用を推進している城北信金から、新たなソフトウェアプラットフォームへ向けられた要求は非常に高いものでした。主要な要件としては、以下のような内容が挙げられました。

- ユーザー単位のパソコン操作履歴取得機能
- 利用者権限に応じた細かな設定機能
- アラートを含めた不正使用の抑止機能

複数のユーザーが1台のパソコンを共有するケースもあるため、ユーザー単位での操作履歴取得が必須でした。さらに、既存の

パソコンOSとして稼働中である Windows 98 Second Edition への対応なども含まれていました。複数のソフトウェア製品を候補として評価作業が開始され、熟慮の末城北信金が選定したのは、インテリジェント ウェイブが提供する情報セキュリティマネジメントプラットフォームCWATでした。



城北信用金庫
システム部 システム企画グループ
次長 濱田 良直氏

「ログ取得、利用の禁止、そして抑止効果、それぞれ

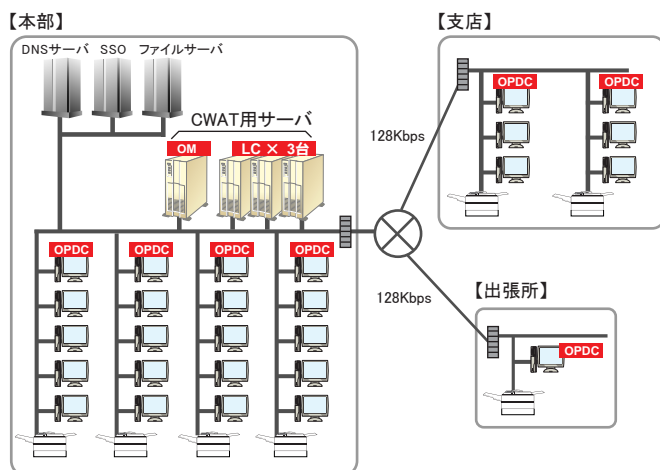
に特化したソフトウェア製品はいくつか存在しましたが、ひとつの製品でこれらすべてを網羅できたのはCWATだけでした」(濱田氏)。

情報漏洩想定試験でも効果がきわだったCWAT

CWATは、機密情報・個人情報の保護に向けた「情報セキュリティマネジメントプラットフォーム」です。機密情報のコピー、印刷、外部メディア書き出しなどのオペレーション監視・制御や、USB、プリンタなどの外部デバイス接続監視・制御などに加え、正常運用時および警告情報発信時の2種類のログを取得することで、「何も起きていないことの証明」、「情報漏洩発生時の証明」などを実現します。さらに、操作中のアラートにより、不正操作の抑止を行うことができます。本番システム導入に先立ち、情報漏洩の発生を想定した試験導入を実施した、システム企画グループ主任の富田祐樹氏は、「CWATの監査ログと他の情報を突合することで、何年何月何日の何時何分に、どのパソコンからの操作で情報がコピーされたか、といったすべての証跡をたどり、最終的に仮定の犯人役を探し出すことができました」その成果を強調しました。

システム概要:全クライアント約1,500台にCWATを導入。すべてのPC操作をトレース

入念な検証ののち、約4ヶ月の構築期間を完了した新システムでは、本部、本支店を含めた全職員が使用する約1,500台のパソコンすべてに、クライアント用ソフトのOPDC(オペレーションディフェンスコントローラ)が導入されました。本部に配備された管理サーバのOM(オーガナイズーションモニタ)を中心とする4台のCWATサーバと監査ログDB用サーバと連携し、職員のすべてのパソコン操作をトレースします。



本部と支店・出張所を結ぶ回線は、128kbpsという比較的回線速度が遅いものだったため、ネットワークに負担がかからないことも要件のひとつとなってしまいましたが、実際の運用を通じて、まったく問題なく稼動することが証明されました。

ユーザー自らの「気付き」、上司への確認帳票出力による確認など、複数レベルでのセキュリティ対応を実現

本システムでは、ユーザーである各職員に対して、その権限に応じた詳細なセキュリティ上の設定を行うことができます。たとえば、一般的なユーザーが情報をFDに書き出そうとすると「その操作はポリシーに違反しています」というアラートが表示され、操作も禁止されます。一方、業務上でUSBへのデータ書き込みが許されているユーザーに対しては、アラートが出るものの、操作は許可されるといった設定が可能です。

「常に見られているという意識が継続するため、不正を行う気がなくなるという抑止効果もあります。さらに、悪意のない操作によるトラブル

もアラートによって避けることができ、紙だけのルールに依存した場合よりも、安心して操作をすすめることができるようになりました」(富田氏)。

さらに新システムでは、これらすべてのパソコン操作の証跡が拠点ごとに帳票として出力され、翌朝店長や上席に提出されます。これにより、前日に発生したすべてのパソコンオペレーションを確認することができます。

ユーザー自らの操作に対するアラートによって「気付く」初期段階での対処から、最終的に出力される帳票確認の段階までを含め、複数レベルでの包括的なセキュリティ対策を実施することが可能となっています。

導入効果:期待した抑止効果が明確に。「CWAT以外では実現できなかったでしょう」

CWATの導入効果について、濱田氏は、「いくつかの要件がありましたが、最も期待していた抑止効果を含めて十分成果が現れたと思います」と語りました。

システム導入以前から、運用によるセキュリティ管理を行い、これらに対する職員の意識も高い城北信金では、「不正による情報漏洩」というリスクよりも、むしろ「故意ではない操作による」リスクの発生が懸念されていました。CWATをコアとする新システムでは、このようなケースでも、不正な操作を実施した際にアラートを表示し、ユーザー本人に知らせることで抑止効果をあげることができます。そして、これらが繰り返されることによる学習効果で、危険性のある操作を次第に減少させていくことが可能となっています。

長年の懸案対象であったパソコン操作監視・抑止及び操作履歴の取得システムを無事実現した濱田氏は、最後に今回のシステム構築プロジェクトを振り返り、「CWAT以外では実現できなかったでしょう」と締めくくりました。



城北信用金庫
システム部 システム企画グループ
主任 富田 祐樹 氏

製品に関する詳しい情報はこちらへ

<http://www.cwatworld.com/>

協力パートナー: 株式会社アイ・ティー・ワン
株式会社野村総合研究所

株式会社インテリジェント ウェーブ

【お問い合わせ】

セキュリティシステム事業部 営業部
〒104-0033 東京都中央区新川1-21-2 茅場町タワー
TEL : 03-6222-7050 FAX: 03-6222-7141
URL : www.iwi.co.jp E-Mail : cwatsales@iwi.co.jp

● 本カタログに記載の会社名および商品名は一般に各社の商標または登録商標です。
● 本カタログに記載されているシステム名、製品名などには必ずしも商標表示 (TM、®) を付記していません。
Copyright © 2006 INTELLIGENT WAVE INC. All rights reserved.