ネットワークから切り離される PC 群に対しても 集中的証拠性保全が可能なシステムの提案

†山中 徹也　*芦野 佑樹　††上原 哲太郎　**吉浦 裕　†佐々木 良一

†東京電機大学大学院 未来科学研究科 情報メディア学専攻
〒101-8457 東京都千代田区神田錦町 2-2
*NEC 共通基盤ソフトウェア研究所
††京都大学 学術情報メディアセンター
**電気通信大学大学院 電気通信学研究科

E-mail：†yamanaka@isl.im.dendai.ac.jp

あらまし　近年, 企業内のデジタル化が進みコンピュータの利用に伴う企業間の訴訟や不正が発生した場合に備え, 端末の操作ログを有事の際の調査や端末監視に活用する様になった. ところが, 既存方法ではネットワークに未接続な端末では適切にログの取得が行えなかった. これに対し芦野・藤田等は独立した環境下で, 端末所持者からの不正にも対応したログの取得が可能な DigForce システムを開発した. しかし, DigForce は常に独立環境下での端末利用を想定した為, 運用が複雑となった. そこで本稿では DigForce にネットワーク管理機能を付加し, ログや管理の自動化・効率化を行い監視システムとしての提案を行う.

Proposal of a system which can intensive evidence preservation for PC group disconnected to network

†TETSUYA　YAMANAKA　#YUKI ASHINO
††TETSUTARO UEHARA　##HIROSHI　YOSHIURA　†RYOICHI　SASAKI

†Graduate School of Science and Technology for Future Life
Information Systems and Multimedia Design, Tokyo Denki University
2-2 Kanda-Nisikicho, Chiyoda-Ku, Tokyo, 101-8457, Japan
#NEC Common Platform Software Research Laboratories
††Academic Center for Computing and Media Studies, Kyoto University
##Graduate School of Electro Communications, The University of Electro-Communications

Abstract　In late years when suit between companies with the use of the computer and injustice occurred because digitization in the company advanced, I came to utilize terminal operation log for investigation and terminal monitor. But, the acquisition of the log was not possible by the existing method adequately at the terminal where unconnected to the network. Ashino and Fujita developed the DigForce system which can acquire the history of operation in the independent environment so that a terminal owner cannot perform injustice. However, the usage became complex because it had assumed DigForce to be use in an independent environment always. In this paper, I add the network management function to DigForce and propose it as efficiency improvement of the log management and a monitoring system that automates it.

１．はじめに

近年, 企業内の情報管理や業務処理のデジタル化が進みコンピュータの利用が増加した. これに伴いコンピュータの利用に関する企業間の訴訟問題や情報漏洩, データ偽装等の不正の可能性に備え, 従業員が利用する PC 端末の操作ログを取得・管理し有事の際の調査や端末監視に活用する様になった. ところが, 従来の方法では管理者が適切に管理を行っているネットワークに接続

していない端末やオフライン等の独立した環境下にある端末では適切な操作ログ情報の取得が行えない等の問題があった.これに対し芦野[1]・藤田[2]等はネットワークに接続できない場所や管理者の手が届かない様な独立した環境下において,例え端末を所持者している従業員自身であっても取得したログに対して不正が困難で適切なログ情報の取得が可能な DigForce システムを開発した.

しかし,DigForce システムは常に独立した環境下でのシステム運用を想定している為,実際に活用する為にはシステムの管理が複雑であり,企業管理者に対する負担も大きいといった問題がある.そこで本稿では DigForce システムに対してネットワークを利用した管理機能を付加し,ログ収集や検証の自動化・効率化とシステム管理の簡易化を図り,新たな監視システムとして提案を行う.

2. 既存ログ監視方式の分類と特徴

端末監視を行う方法は操作ログを取得するロガー機能とログデータの保存・管理を行うログストレージ機能の設置場所により下記表 1 に示す様にネットワーク監視型とスタンドアロン監視型に分類できる.

表 1　監視型の分類

機能＼監視型	ネットワーク監視型	スタンドアロン監視型
ロガー機能	ユーザ端末内部	ユーザ端末内部
ログストレージ機能	管理サーバ	ユーザ端末内部

2.1 ネットワーク監視型（NT 型）

ネットワーク監視型とは図 1 に示す様にユーザ端末内に操作ログの取得を行うロガープログラムを導入する.そして企業 LAN 内に置かれた管理サーバと通信しながら,操作ログが取得された場合には逐次管理サーバに対しログデータを転送する事で,ユーザの操作ログへの不正を困難にすると共に,不正を検知した場合には中央のサーバからユーザ端末に対して制限をかける事で即時の対応が可能であり,管理サーバでの一括した端末の管理と監視が可能である[3].

しかしこの方法では常に社内 LAN に接続していなければログの収集・活用が行えず,社外に持ち出したりオフライン等で利用されている端末に対しては正当性の確保されたログが取得できない等の問題がある.

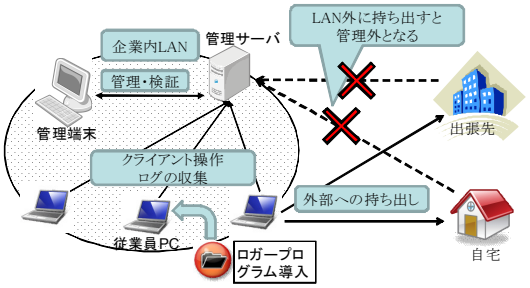

図 1 ネットワーク監視型

2.2 スタンドアロン監視型（SA 型）

ネットワーク監視型では困難であった独立した環境下において正当性を確保しながら操作ログを取得する方法にスタンドアロン監視型がある.これは芦野[1]・藤田[2]らによって開発された DigForce システムをログ収集を行う為の監視・制御プログラムとして端末に導入し, 図 2 に示す様に補助デバイスに蓄積されたログを定期的に管理者が回収する事で端末利用状況の把握・監視を行う方法である.

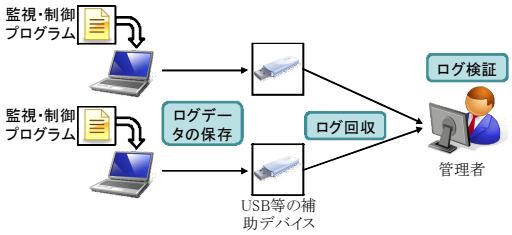

図 2 スタンドアロン監視型

2.2.1 DigForce システム

DigForce システムとは下記 2 つの機能を主として持ち,スタンドアロン環境下において端末所持者であってもログに対する不正を困難にしたロガー・ログストレージプログラムである.

機能 1：Shielded-Chain 方式ヒステリシス署名を用いた操作ログ取得機能

機能 2：ホワイトリスト方式によるアプリケーション起動制御機能

(1)機能 1 とは,取得される操作ログとあらかじめ管理者によって設定された連鎖データを組み合わせて署名を取るヒステリシス署名に,署名の繋がりを保証する連鎖データを耐タンパ領域に保存する仕組みを用いる事で端末所持者からの不正に対処し,正当性が確保された署名を取得する方法である.

この方法は図 3 に示す様に初期連鎖デ

ータ n=1 とログデータ n=1 を合わせて署名 1 を作成し,署名 1 を元にさらにハッシュを取得し連鎖データ 2 とする,そして次に取得されたログデータ 2 とあわせて順次署名を作成する方法で,連鎖データを Trusted Platform Module (TPM) 内で管理する事により端末所持者であっても保管されたデータに対し不正が行えず,ログの連鎖構造を検証する事により独立した環境下で取得されたログでも不正検知が可能で正当性の確保されたログの取得が可能となる.

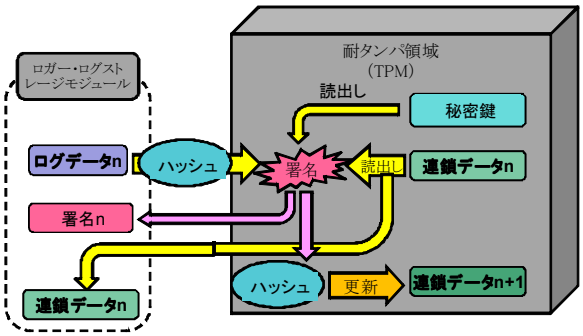

図 3 ヒステリシス署名の流れ

(2)機能 2 とは, 図 4 に示す様に PC 端末上で起動するプログラムを常に起動監視プログラムに監視させ, プログラムが実行される際に管理者が起動を許可したプログラムのハッシュ値一覧リスト(=ホワイトリスト)とを照合し,ホワイトリストに登録してあるプログラムのみ起動を許可し, その他のプログラムの起動を制限する機能である.これにより端末上でログ取得プログラムに対し不正を行うプログラムや業務上利用が好ましくないソフトウェアの起動を禁止させることができる.

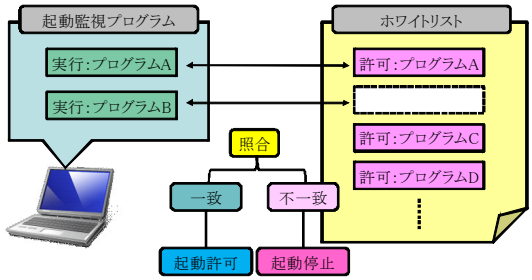

図 4 プログラム起動制御機能

2.3 DigForce システムの問題

ネットワーク監視型では不可能であった独立した環境下での適切なログの取得とそれを元にした監視も DigForce をベースとしたスタンドアロン監視型を活用すれば可能となる.

しかし,現在の DigForce には下記の様な問題がある.

問題１：デバイス回収問題

現在の DigForce ではログデータを保存した補助デバイスと TPM に連鎖データ等が保存された PC 本体を企業管理者が個別に回収し,個々に検証プログラムを実行して検証を行う必要がある.その為,ログデータの取得から検証までに大きな時間の空きが存在し,不正が起きていた場合に対処が遅れる可能性がある問題である.

問題２：設定更新問題

設定更新の問題とは現在のシステムにおいて運用途中で許可プログラムの更新を行うには利用中の端末を一度回収し,ホワイトリストの状態確認と変更を管理者が行う必要がある.その為,運用途中で不正に関与する可能性があるプログラムを発見しホワイトリストを更新したとしても,端末が外部で利用中である場合には更新の適応が適切な時間内に行えない問題である.

問題３：管理者負担問題

デバイス回収や設定更新の問題に関連し,現在の DigForce システムではログの回収や設定更新の際に管理者が直接端末に接触し,個々の端末で各操作を行う必要がある.その為,複数台の端末でこのシステムを導入し端末の監視を行おうとすると管理者に対し検証や設定変更の為に多大な労力や時間コストが必要となる問題がある.

次章では以上の問題にネットワークを利用した管理機能を付加する事で対応しログ管理の自動化・効率化とシステム管理の簡易化を図った監視システムの提案を行う.

3 システムの提案

3.1 システム関与者の定義

提案に際し関与者を以下の様に定義する.

- システムの開発・提供企業･･･ベンダ C
  - システムの管理者･･･ベンダ A
- 監視システムの利用企業･･･ユーザ C
  - 利用企業の責任者･･･ユーザ A
  - 利用企業の従業員(端末の利用者)･･･ユーザ U

3.2 前提条件

提案システムの前提条件は以下の通りとする.

条件 1：ベンダ A は管理サーバにおいて不正を行わないものとする.

条件 2：管理サーバ稼働時や制御プログラム導入時に不正は無いものとする.
条件 3：ユーザ A やユーザ U はベンダ C にログが管理される事を承認しているとする.
条件 4：ユーザ U は管理者権限のないアカウントで PC 端末を利用する.

3.3 問題への対応

提案システムでは 2.3 節にて述べた問題について表 2 に示す機能,構成の追加を行い,既存システムの自動化・効率化と管理の簡易化の実現する.

表 2 問題と対応策

問題		対応策	
Q1	デバイス回収問題	A1	ネットワーク認証機能の追加
		A2	ログデータ転送機能の追加
Q2	設定更新問題	A1	ネットワーク認証機能の追加
		A3	管理サーバとの更新機能の追加
Q3	管理者負担問題	A4	SoftwareAsAService(SaaS)としての運用と構築

対策：A1 ネットワーク認証機能の追加

ネットワーク認証機能は端末の起動時・終了時等にネットワーク接続の有無を確認し,接続が確認された場合は端末の認証とオンライン時の処理を,接続が確認できない場合はオフライン時の処理を DigForce に行わせる機能である.

図 5 に処理の流れを示す.

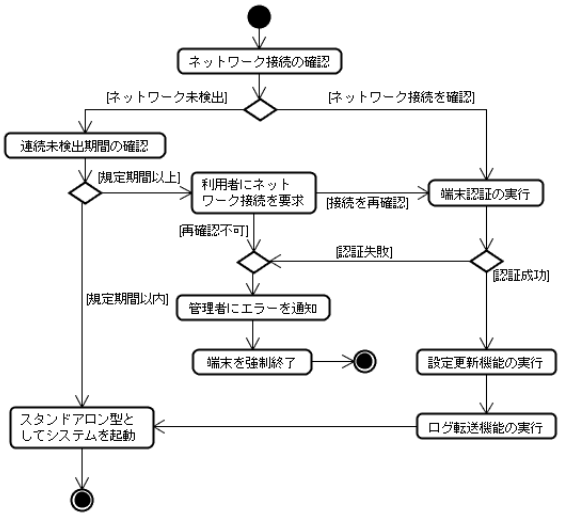

図 5 ネットワーク認証フロー

対策：A2 ログデータ転送機能の追加

ログデータ転送機能はネットワーク認証機能によりネットワーク接続が確認された場合に端末で取得・保管されたログデータと検証用の連鎖データを自動的に PC 端末からサーバにアップロードする機能である.

対策：A3 管理サーバとの更新機能の追加

管理サーバとの更新機能とはホワイトリストや設定情報等の更新を行う際にサーバに保管された端末の設定情報と実際の端末の設定情報を比較し変更が確認された場合に,その更新内容を端末へ適応させる機能である.図 6 に手順を示す.

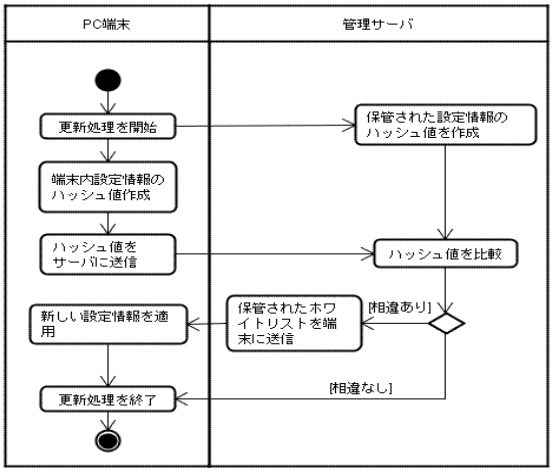

図 6 更新機能フロー

対策：A4 SaaS としてのシステムの構築

SaaS としてのシステムの構築とは 3.4 節で説明する構成にてシステム実装し,提案システムの管理機能をユーザ側ではなくベンダ側で委託管理し,利用企業は監視情報の設定や取得されたログデータを管理サーバに送り利用する事で,システム管理や運用にかかるコストの削減を行うものである.

システムを個別に構築せずログをベンダサーバで管理する SaaS の構成には以下のメリットがある.

① システムの管理・維持コストを軽減できる.
② 専門的なセキュリティ知識を持った管理者によるシステムの管理,運用が行え,利用者はシステムを利用するだけで良い.
③ PC 端末内のディスク容量をログに割かずに済み,端末に問題が発生してもログの検証が可能である.

3.4 システム構成

提案するシステムの構成は図 7 のようになり下記 3 つの要素により構成される.

- 構成要素
  - ログ収集・端末制御用プログラム

(DigForce)を導入したPC端末
- プログラムの管理・更新やログの収集・検証を行う管理サーバ
- 使用状況確認の際に企業管理者が利用するウェブブラウザ

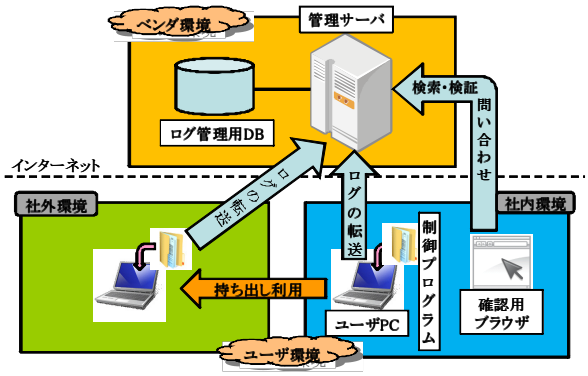

図 7　提案システムの構成

3.5　システムの運用

3.5.1　導入フェーズ

初回導入時は図 8 に示す手順でユーザ A が端末を確認したうえで必要な情報をサーバに登録する. そしてサーバでの設定が終わると監視に必要な情報が端末にダウンロードされ完了となる. その後端末はユーザ U に渡されて監視下で端末を利用する利用フェースへと移る.

以下に図 8 の各手順の詳細を示す.

(0) ベンダ C とユーザ C が業務内容からホワイトリストの候補となるハッシュを登録しておく.
(1) ユーザ A が PC 端末に不正なプログラムが導入されていないかを確認する.
(2) 監視・制御用プログラムをインストールする.
(3) ユーザ A が管理サーバへユーザ名，企業情報，端末情報等を送りユーザの登録を行う.
(4) 管理サーバがデータベースにユーザ情報, ログ収集・管理情報の登録を行う.
(5) 管理サーバが登録された企業情報を元にデータベースから許可プログラム情報の検索・収集を行う.
(6) 管理サーバが確認された許可プログラム情報からホワイトリストファイルを作成する.
(7) 管理サーバからホワイトリストを端末へダウンロードする.

以上の手順にて初回設定を完了すると，ユーザ A からユーザ U に端末を渡しホワイトリストにそった監視下で端末が利用されるようになる(図 8-(8)).

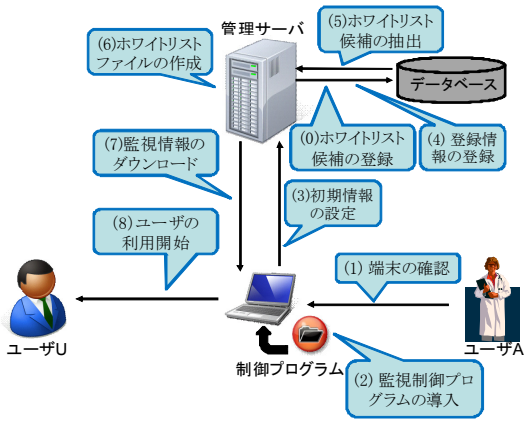

図 8　導入フェーズ

3.5.2　利用フェーズ

導入フェーズが完了した状態で端末を起動すると，制御プログラムがネットワーク接続状況の確認を行い, ネットワーク接続の有無により下記の 2 つのパターンで端末の起動制御とログの取得・管理を行う.

(以下に各パターン毎の詳細手順を示す)

パターン１：ネットワークへの接続を検知できなかった場合(図 9)

(0) 端末が起動時にネットワーク認証機能を使いネットワーク接続を確認する.
(1) 端末が一定期間ネットワークへ接続せず利用されている場合, ユーザ U に対しネットワークへの接続を促し期間が一定値を超えるとネットワークへ接続しない限り起動制限をかける.
(2) 端末で制御プログラムをスタンドアロン監視型として実行させる.
(3) 制御プログラムが端末内で操作ログの取得を行い次にネットワーク接続が確認されるまで端末内に保管する.

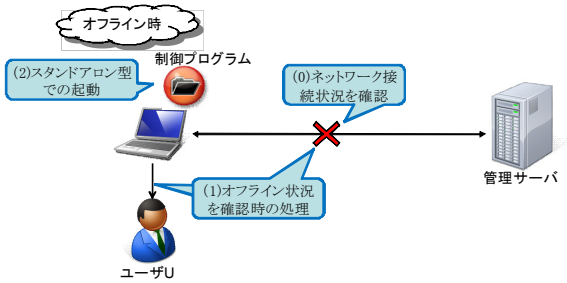

図 9　独立した環境下での利用

パターン２：ネットワーク接続を検知できた場合(図 10)

(0) 端末が起動時にネットワーク認証機能を利用しネットワーク接続状況を確認する.
(1) 接続状況確認後, ログ転送機能により

管理サーバにログを転送する.

(2) 管理サーバが転送されたログからインデクス情報を抽出し検索・検証時が行える様にデータベースに登録する.

(3) 更新機能によりホワイトリストが適切な状態か確認し,変更があれば新しいホワイトリストを端末にダウンロードし適用させる.

(4) 制御プログラムがサーバへの転送処理後,古いログデータを削除する.

(5) 端末でスタンドアロン監視型として制御プログラムを実行させる.

一定の時間間隔毎に(1)～(5)を繰り返し周期的にログをサーバへ転送する.

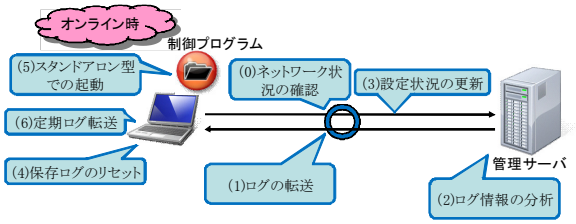

図 10　オンライン環境での利用

3.5.3　管理フェーズ

起動制御を行う為のホワイトリストを変更する場合，word や excel 等の一般に広く普及しているソフトに関してはベンダ A が定期的にデータベースのハッシュ情報を更新する.またユーザ側で独自に開発･利用している専用ソフト等のベンダ A では情報を入手できないソフトに関してはユーザ A に専用のホワイトリスト作成プログラムを渡しておくことで，必要に応じて登録情報の更新をユーザ A に行ってもらう.

(詳細手順を図 11 と共に下記に示す.)

(1)ベンダ A 又はユーザ A が持つホワイトリスト作成ソフトにより信頼するプログラム実行ファイルからハッシュ値をとる.

(2)取得したハッシュをデータベースに登録しホワイトリスト候補となるソフトウェア情報を更新する.

(3)管理サーバと PC 端末がネットワーク接続確認を行った際に変更を確認し,変更があれば新規ホワイトリストを端末にダウンロードし更新を反映させる.

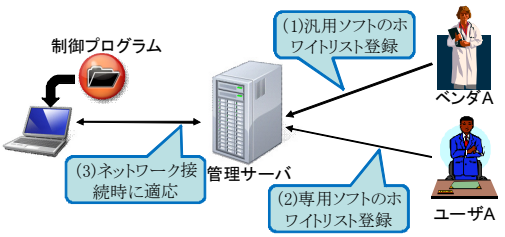

図 11　管理フェーズ

3.5.4　検証フェーズ

利用確認を行う場合は，ユーザ A が管理者アカウントで専用ページにログインし，ブラウザから検索条件を入力し問い合わせを行う．管理サーバでは検索条件により該当するログ情を抽出し，不正の検証を行った上でユーザ A に対し結果を開示させる.

その手順の詳細を図 12 と下記に示す.

(1) ユーザ A が閲覧者用アカウントで専用ページにログインし検索条件を入力する.

(2) ユーザ A がウェブブラウザを通じ管理サーバへ問い合わせを行う.

(3)管理サーバがデータベースから検索条件に該当するログを検索する.

(4)管理サーバが条件に該当するログを抽出しそのログの署名情報の検証を行う.

(5)管理サーバが検索結果をユーザ A にブラウザを通じ開示する.

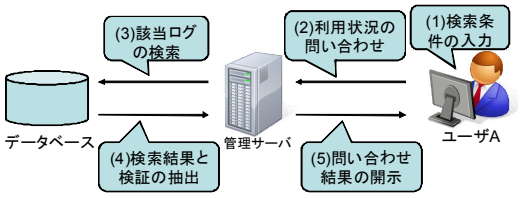

図 12　検証フェーズ

4　おわりに

本稿では DigForce をベースにネットワーク管理機能を付加する事でログ収集の高速化・自動化とシステム管理の簡易化を図った監視システムの提案を行った.今後はサーバ側に対する不正を含めた対処と機能・性能評価を行う予定である.

参考文献

[1] 芦野 佑樹; デジタルフォレンジックシステムにおける証拠保全方式の開発に関する研究，博士論文，東京電機大学 先端科学技術研究科 情報メディア工学専攻，2009

[2] 藤田 圭祐，芦野 佑樹，上原 哲太郎，佐々木 良一; 不正プログラムの起動制御機能を持つDFシステムの提案，情報処理学会コンピュータセキュリティシンポジウム 2007 (CSS2007) 論文集 CD-ROM，2007.11.2

[3] Yuhua Qin ; “The Development of Monitoring Software for Local Area Network”, Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control (ICICIC 2008), Volume 00, Pages 379 - 382, (2008).