在宅勤務の労務管理にも役立つＰＣ操作ログ監視導入で大切な5つの事

2018/12/26

2014年7月に発覚した通信教育業大手B社の顧客情報大量流出事件はまだ記憶に新しいところと思います。同社関連システム会社の派遣社員が約3000万人分の顧客データベースを自身のスマートフォンに書き写し名簿業者に売却していたもので、他の企業から送られたDMに関する問い合わせが多数寄せられたことで事件は明るみに出ました。B社はこの事件に対処するためにお詫びの金券に総額200億円の出費、その後の1年間で約90万人の会員流出、2期連続赤字計上など、甚大な損害を被ることとなりました。個人情報をはじめとした情報漏洩事件がひとたび起こってしまえば、企業の屋台骨を揺るがしかねないという教訓を教えてくれました。

『2017年情報セキュリティインシデントに関する調査報告書』(*)によりますと個人情報漏えいの媒体・経路の調査結果においてPC（パソコン）が流出源と見られる項目の合計は57%にもなります。意識的に行われる不正行為にしても、無意識のうちに流出してしまうトラブルにしても、その半分以上は社員のPCが情報漏えいの根源となっているのです。タイトルにあります「PC操作ログの管理は必須」の主張の一番の根拠はここにあります。

　本記事ではPCの操作ログとは何なのか、その管理が今いかに求められているのか、管理システム導入でどのような効果が得られるのか、システム導入におけるリスクはないのかなど、AtoZを分かりやすくお伝えします。ログ管理システム導入への一助にしていただければ幸いです。

＊NPO日本ネットワークセキュリティ協会の2018年6月公表の調査

目次

1. PCの操作ログとは？

「ログ」とはコンピュータの操作内容や通信、サーバーへのアクセスなどの履歴のことを指します。具体的には下記のような操作すべての履歴のデータがファイル化されています。

・電源ON・OFF　　**・サーバーアクセス**

・使用開始（ログオン・ログイン）　　**・Ｅメール送信・受信**

・使用終了（ログオフ・ログアウト）　　**・Web閲覧**

・印刷（プリントアウト）　　**・ソフトウェアやファイルのダウンロード**

・アプリケーション起動　　**・ファイル作成・編集・削除**

・ソフトウェアのインストール　　**・外部記録媒体接続**

・ソフトウェアの自動アップデート　　**・スパイウェアの侵入**

社員が毎日業務で使用しているパソコンであれば、これらのログファイルが日々集積されていくとたちまち膨大なデータ量になってしまいます。そこで、そのパソコンの能力によっても差がありますが、一定期間を経過すると過去のログは上書きされていく仕掛けになっています。このため何の対策もせずに社員のPCの操作ログを管理しようとすると、各PC上での確認作業が必要になり、しかも古いログは上書きされていて確認できないことになります。

2. なぜ企業経営に『PC操作ログの管理』が求められるのか？

昨今の情報セキュリティ対策への要求は、企業の大小や業種・業態に関わらずどんな法人に対しても突き付けられてきています。従来、ネットワークやシステム、ウィルス対策に重点が置かれていましたが、情報漏洩事件の頻発する状況下、従業員個々のPCにまで対策が求められてきています。その包囲網は確実に全方向から狭められてきています。

2-1. 情報セキュリティリスクの高まり

企業や組織の運営において情報システムやインターネットは今や無くてはならない存在となっています。しかし、その利便性の向上と引き換えに、その扱いを誤れば経営の根幹を揺るがしかねない大きな危険性を抱え持つことになりました。特に情報セキュリティに対するリスクマネジメントは重要な経営課題のひとつと考えなければなりません。個人情報や顧客情報などの重要情報を取り扱う場合には、これを保護することは、企業や組織にとっての社会的責務でもあります。この責務を全うするための重要なツールとして「PC操作ログの管理」が求められてきています。

2-2. 働き方改革・テレワークの広がり

70年ぶりの労働法大改革となる「働き方改革」一括法案が2018年6月29日の国会で成立しました。残業時間の上限規制が法制度化され、長時間労働の是正に向けた取り組みが進んでいます。また多様で柔軟な働き方の実現に向けてテレワーク制度の導入にも注目が集まっています。オフィス以外の自宅や出張先などでフレキシブルに就業できる環境がどんどん広がりつつあります。しかし、こうした就業環境を野放しにすれば就業時間の管理はまったくできないことになってしまいます。少なくともPC操作ログの遠隔管理が為されなければ、テレワークの管理はできません。

2-3. 法的規制、政府の指導の強化

2006年成立した金融商品取引法（俗称：日本版SOX法）において、内部統制の有効性を継続的に監視・評価するプロセス（モニタリング）とITの利用を求められ、この求めによりログの収集保存と分析ができるシステムの導入が必要とされました。この法律に従い多くの上場企業では既にPC操作ログの管理システムの導入が進んでいます。非上場企業、中小企業はこの時点ではこうした管理システムへの関心は盛り上がらずに10年近くの年月が経過しました。しかし2017年5月に個人情報保護法が改正されてにわかに状況が変化してきました。同法の改正で、大半の法人が「個人情報取扱事業者」とされることになり、そのガイドラインでは「ログ等の定期的な分析により、不正アクセス等を検知する」といった指針が盛り込まれてPC操作ログの管理が求められるようになっています。

2-4. 取引先の情報セキュリティ要求度の高まり

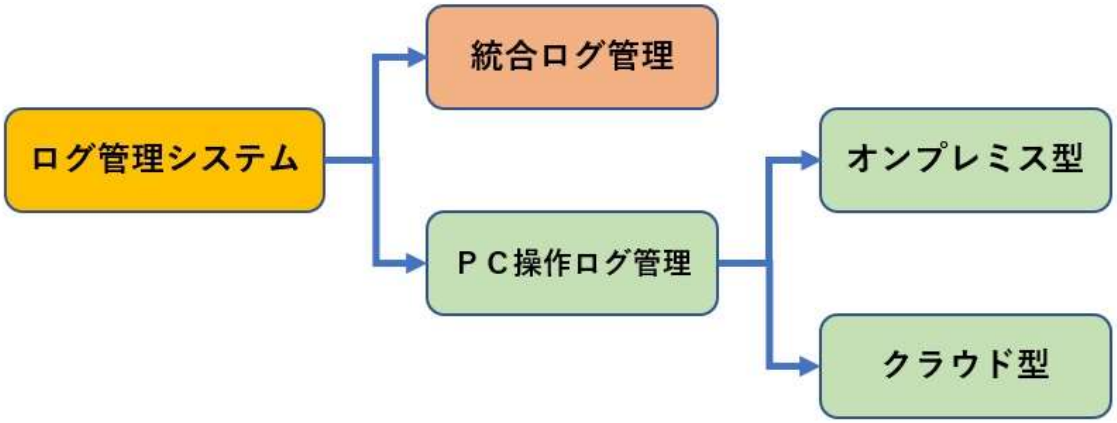
プライバシーマーク取得企業や個人情報取扱事業者が業務を外部に委託する際、その業務内容が顧客情報や個人情報の加工、業務システムの開発、データの開示を伴うアウトソーシングなどである場合、委託先企業に対して求められる情報管理レベルは依頼者と同等のものが要求されることは自然な流れです。事実、筆者の所属する会社でも銀行や保険会社、上場大手メーカーなどの取引先から受ける情報セキュリティの監査で入退室、書類の保存状態、個々のPCの基本的なセキュリティなどに加え、操作ログの管理を求められるケースが増えつつあります。総務省や関連法律のガイドラインでは、中小零細企業に対してログの管理システム導入までを求めているものはまだありませんが、取引先など民間レベルにおいては徐々にその要求度は高まりつつあります。

3. 操作ログ管理とはどういうものなのか

何十人、何百人と社員がいる法人で1台1台のPCで操作ログファイルを確認し管理するのでは、管理者にいくら時間があっても足りませんし現実的ではありません。その問題を解決するために作り出されたのがPC操作ログの管理システムで、管理者のPCで社員のPCの操作ログを一元的に管理できる便利な仕掛けです。まずはその上位でネットワーク機器類の管理をするシステムを含め、ログ管理システムを俯瞰してみます。

3-1. ログ管理システムの種類

ログ管理システムは様々な種別がありますが、PC関連のログに限る場合、大きく以下のように分けられます。



3-1-1. 統合ログ管理

ファイアウォールなどのセキュリティ機器、プリンターやネットワーク機器、サーバーやデータベースのシステムログ、PCのWebアクセスやメールといった様々な機器のログを統合データベースにまとめ、一括して管理できるツールのことです。クライアントPCの操作ログを取り込む機能を持つ製品もあります。統合ログ管理ツールはパッケージソフトウェアによる提供が主体で、最近広がりつつあるSaaS型はまだ汎用的にはなっていないようです。

統合ログ管理はネットワーク全体を俯瞰して管理することを主要な目的として開発されたもので、大規模な企業やセキュリティリスクが高い企業を中心として導入されています。

本記事は端末PC操作ログ管理の重要性をお伝えするものなので、統合ログ管理のご説明はこの程度に留めさせていただきます。

＜主な製品＞

3-1-2. PC操作ログ管理

製品名	メーカー	特徴
Logstorage	インフォサイエンス	ネットワークに繋がるあらゆる機器類のログを大量に取り込みできることを強みとする【中堅～大手企業向け】
LogRevi	インテック	
LogAuditor	三菱電機インフォメーションテクノロジー	
Alog	網　屋	ファイルサーバーログ収集に特化【中堅～大手企業向け】

主にクライアントPCの操作ログを中心としたログ管理ツールです。セキュリティ対策の操作ログ以外に、インベントリ情報といったPC管理に必要な情報の収集機能も搭載しています。クライアント運用管理ツールは大きく分けて以下の2つの提供形態があります。

1）オンプレミス型（パッケージソフト）

「オンプレミス」とはシステム構築に必要なサーバー機器などを利用者側で導入し、運用することをいいます。社内に操作ログ専用サーバーを用意して運用する構成となります。最近ではMicrosoft AzureやAmazon Web Serviceなど、クラウド上に構築するケースも出てきました。導入される専用サーバーの容量にもよりますが、ログの長期保存に向いています。パッケージソフトウェアのため買い切りで初期投資額は大きくなります。次年度以降は保守費用のみである場合が多く、ランニングコストは安価になります。ただし、サーバーのメンテナンス・管理が必要なため、サーバー管理者などを配置できる情報システム部門などがある企業向けです。

2）クラウド型（SaaS）

導入社内に専用サーバーを用意せず、製品提供元が用意しているクラウドサーバーを利用する構成です。サーバーの管理は製品提供元が行うためサーバー運用の手間は不要です。専用のソフトウェアを管理すべきPCにインストールするだけで、初期投資をほぼゼロに抑え、素早くログ管理を始めることができることが最大のメリットです。反面、システムや機器の構成に対するカスタマイズへの対応がされにくいというデメリットがあります。また、クラウド上のサーバー容量には制限がありますので、数ヶ月程度で収集したログを消去するか、バックアップを取る作業が求められます。コスト面では、月額または年額で固定費用が発生するため、利用年数が増えるにつれ、ランニングコストはオンプレミス型に対して高くなる傾向があります。

＜主な製品＞

提供形態	製品名	メーカー	特徴
オンプレミス型	MaLion	インターコム	操作性・分かり易さに重点を置き開発され、インベントリ収集とPC操作ログ収集を主機能としている【中堅～大企業向け】
	LanScopeCat	MOTEX	
	SKYSEA	SKY	
	Systemwalker	富士通	リソース管理を含めPCやサーバーの運用全般に重点を置き開発されている。【大企業向け】
	JP1	日立製作所	
	Mcore	住友電工情報システム	
クラウド型	MaLionCloud	インターコム	サーバー運用管理者がいない企業でも容易に導入・管理ができるように開発。【～300台程度までの中小企業向け】
	ISM Cloudone	クオリティソフト	

3-2. PC操作ログ管理システムの基本的な3つの機能

メーカーの仕様により優劣はありますが、どのシステムでも大別すると以下の3つの機能を備えています。

3-2-1. PC操作ログの保存と監視

1章にありました各社員PCの「操作ログ」を長期的・一元的に保存・管理することで、トラブルや不正行為が発生した時に、その原因が「誰のPCで」「いつ起こったか」を検証・確認するための機能です。予め決められた操作や動作に対して管理者へのアラートを即座に発するなどの設定も可能で、問題の拡大を最小限に留めることが期待できます。

3-2-2. PC操作への警告と制御

「行ってはならないコピーやプリントアウト」「就業中の禁止サイトの閲覧」「使用禁止の記憶メディアの接続」などに対して、その発生を未然に防ぐために各PCに対して警告を発したり、操作そのものを制御したりする機能です。こうした機能を積極的に活用することで、より能動的に情報漏えいや禁止行為を未然に防ぐことができます。

3-2-3. ハードウェアやソフトウェアの管理機能（インベントリ情報の収集と管理）

数十台、数百台というPCになってきますと、資産管理という観点でもその管理は非常に煩雑で追跡が困難になり、エクセルなどの表計算ソフトでの手入力管理にもすぐに限界が来てしまいます。こうした面倒な作業をPCログ管理システムでは一元管理をすることができます。機器類のハードウェアの管理もさることながら、ソフトウェアの管理はもっと重要です。ソフトウェアの違法コピーは著作権法により厳しく罰則が定められており、一歩間違えると企業経営の命取りになりかねない問題で、ログ管理システムでは、導入したソフトウェアやそのライセンスを管理者PCで一元管理をすることができるのです。

＊インベントリとは：
もともと「目録」「保有資産」という意味で、IT用語としてはネットワーク上に接続される機器の機種、MACアドレス、IPアドレス、CPUの型番やメモリ、ハードディスク容量、利用履歴などの情報のことを指します。

4. PC操作ログ管理システム導入成功への5つのポイント

PC操作ログ管理システム導入に際して、技術的・システム面での注意点や使い方などは各メーカーがしっかりと情報発信していますのでそちらにお任せするとして、ここでは管理システム導入への考え方、運用ルール、心構えなどソフト面について大切なポイントをお伝えします。

4-1.「情報漏えい対策」は導入の目的に必ず加える

2章でも説明しましたとおり、法人の経営において個人情報取扱事業者としての情報漏えい対策は必須です。『個人情報保護法など法規制によって』、『総務省など政府機関のガイドラインによって』、あるいは『取引先からの情報セキュリティ対策要求によって』など、多方面からの情報漏えい対策への要求度の高まりにより、PC操作ログの管理システム導入は早晩進めなければならなくなります。Web閲覧の監視や制限、勤労管理上のログオンログオフのコントロール、IT資産の継続的管理など他の目的でシステム導入を検討される場合でも、**必ず情報漏えい対策と抱き合わせて導入するべきです。**

4-2. 操作ログを保存するのか、操作そのものを制御するのか

■ 操作ログを収集・保存し何か問題が起きた時に状況把握をする目的で使うのか

■ 何か問題が起こる前に未然に防ぐために積極的に操作を制御するのか

その目的によって、システム導入への取り組みも大きく異なってきます。導入の前提としてそのスタンスを明確にされることをお勧めします。もちろん問題は起きないにこしたことはありませんが、それを恐れて何でもかんでも「アクセス禁止」にしたり、規定時間で「強制ログオフ」にしたり、あらゆるアクションに警告を発したりすれば、現場は確実に混乱と困惑に陥ります。また、「経営は社員を全く信用していないのか？」といった猜疑心を生み、組織全体がギクシャクした状況になってしまうリスクもはらみます。この匙加減・バランス感覚がPC操作ログ管理導入の成否を分けるかもしれません。

4-3. 就業規則への明記と導入告知は必ず実施

PC操作ログの管理システム導入は、従業員のPC操作を常時監視（モニタリング）することとほぼ同義です。従来、私用のＥメールやWeb閲覧に目をつぶっていたとしますと、そうした個人の私信や行動まで覗き視ることになります。就業時間内での私用のPC操作は服務規則に違反する事になりますので、こうした行為をモニタリングで管理することは就業規則上問題とはなりませんが、**「プライバシーの侵害」という側面ではセンシティブな問題をはらみます**。こうした事案で労使間に無用な軋轢を生じさせないために、以下の4つの点を留意することが肝要です。

Ⅰ. モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。

Ⅱ. モニタリングの実施に関する責任者とその権限を定めること。

Ⅲ. モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程を策定するものとし、事前に社内に徹底すること。

Ⅳ. モニタリングの実施状況については適正に行われているか監査、または確認を行うこと。

4-4.「自動レポート作成で管理の省力化を諮ることが肝要

PC操作ログの管理システムは非常に多機能で優れた仕掛けです。しかし、多機能であるが故に従来ならあきらめていた様々なPC操作管理をできるがために、管理項目が増えすぎて責任者への負担が非常に増してしまう恐れがあります。ただし、大半のメーカーのシステムには自動レポート作成機能があります。これを上手く活用することで管理の省力化を諮ることが可能になります。日報では何を掲示するのか、週報ではどのような項目をチェックすべきか、即時のアラートを必要とする事象は何かなど、導入する際に周到に計画して、運用が始まればトライアンドエラーを繰り返して、その企業のオリジナルの管理手法を構築する必要があります。

4-5.「経営者が「のぞき魔」にならないこと

社員のPCにおける一挙手一投足が監視できてしまう・・・・・。
悪意ある人がこのツールを手にすれば、必然的に起こることは想像に難くありません。

それが万が一企業の経営者であった場合、管理責任者に圧力をかけルールを逸脱しても社員の行動をのぞいてしまうようなことが起きかねません。一度このような事が起こればその後の歯止めが効かなくなり、健全な企業経営は風前の灯に向かう事になるでしょう。

「経営者が悪人」というような極端なケースはわずかだとしても、経営者心理が「性善説」と「性悪説」の間で揺れ動く中で、特定の社員のPC操作をチェックすることは十分考えられることですし、ここまでならさして問題にはなりません。しかし、この行為がエスカレートしてその社員の一挙手一投足を覗き見てしまうことになってしまえば、プライバシーの侵害となり経営モラルの逸脱と捉えられても仕方がありません。そして「社長は社員のPCをいつも覗いている」との風評が社員の間に広がってしまえば、築きあげてきた信頼関係は一瞬のうちに崩れ去ることでしょう。特に「社長がルールだ」となっ てしまいがちな中小のオーナー色の濃い企業では、こうした問題が起こってしまう可能性が高くなります。

PC操作ログの管理システムを導入するにあたり、**経営者が「社員のプライバシー保護」を遵守し制定されるルールに従う誓いを立てること**が、システム運用成功への第一歩となるはずです。

5. まとめ

PC操作ログ管理は、企業規模や今あるインフラに合ったシステムを選定し予算化すれば、その導入は物理的にはさして難しいものではありません。片や「導入を社員に告知するのか？」「社員が疑心暗鬼にならないのか？」「ルール作りはどうしたらいい？」「管理の仕方は？」などソフト面で乗り越えなければならないハードルが少なからずあります。この記事を読まれるあなたの会社は、こうした面倒なことを言い訳にして導入に踏み切れていないのかもしれません。しかし、今日の情報セキュリティへの取り組みの各方面からの要求はすでに「待ったなし」の状況になっています。あなたの会社が未だ「PC操作ログの管理」をされていないならば、その導入の検討は喫緊の経営課題です。