進化する明日へ Continue thinking

I-O DATA

ホワイトペーパーシリーズ：

追加コストなし！中小企業で可能な、LAN DISK H の情報セキュリティ対策

2016 年 9 月

内容

本文書は、株式会社アイ・オー・データ機器（以下、「アイ・オー・データ」とします。）が、アイ・オー・データの特定の商品に関する機能・性能や技術についての説明を記述した参考資料となります。当該商品の利用という目的の範囲内で自由に使用、複製をしていただけますが、アイ・オー・データの事前の書面による承諾なしに、改変、掲示、転載等の行為は禁止されます。また、**あくまで参考資料として提供いたしますので、内容については一切保証を致しかねます。**以下の内容をご了承いただいた場合のみご利用ください。

(1) アイ・オー・データは、本文書によりいかなる権利の移転もしくはライセンスの許諾、またはいかなる保証を与えるものではありません。

(2) アイ・オー・データは、本文書について、有用性、正確性、特定目的への適合性等のいかなる保証をするものではありません。

(3) アイ・オー・データは、本文書を利用したこと、または利用しなかったことにより生じるいかなる損害についても責任を負うものではありません。

(4) アイ・オー・データは、本文書の内容を随時、断りなく更新、修正、変更、削除することがあります。最新の商品情報については、http://www.iodata.jp/ をご覧ください。

1. 概要

標的型攻撃による組織内部へのサイバー攻撃や、内部不正による情報漏えいの問題が市場を震撼させています。さらに、最近ではランサムウェアによる企業内の重要データの被害と、セキュリティインシデントが後を絶ちません。情報セキュリティ対策の重要性は増す一方ですが、企業によっては専任者がおらず、コストが掛けられないため、効果的な対策が難しい場合もあります。

本ホワイトペーパーでは、追加コストをかけない NAS の情報セキュリティ対策について説明いたします。まず、NAS の情報セキュリティ対策の必要性についての解説を行い、次に LAN DISK H で可能な対策について解説します。最後に内部不正に効果的なアクセスログ運用の実例をご紹介いたします。

2. 背景

2.1 企業で NAS を利用するメリット

企業で NAS が活用されるケースが増加しています。2013 年の Windows XP のサポート終了により、多くの XP 端末の買い替えが発生し、企業で利用される高性能なパソコンが増加しました。その結果、企業内で作成される電子データも増加しています。電子データが増加すると、データのやりとりを効率よく行う必要が出てきます。この課題を解決するのが LAN 接続型ハードディスクの『NAS』です。

企業において、重要なデータは社内に保存したいが、サーバーまでは不要なケースも多いと思われます。そこで NAS が注目されています。

2.2 情報セキュリティ対策の必要性

内部不正による情報漏洩や、標的型攻撃によるサイバー攻撃など、セキュリティインシデントの話題が大きな社会問題となってきました。さらに 2016 年 3 月よりランサムウェアによる被害が爆発的に広がるなど、セキュリティインシデントの拡大はとどまることを知りません。

一方で、マイナンバー法施行により、平成 27 年 10 月より日本国内の全住民にマイナンバーが通知され、全事業者に対して安全管理措置が課せられるなど、法令対応も必要となってきました。今後も様々な法令改正の中でさらに情報セキュリティ対策が求められるものと思われます。

また、昨今では自社内のポリシー設定だけにとどまらず、親会社や取引先からも情報セキュリティ対策を求められるようになってきており、ますます負荷が高くなってきています。

2.3 NAS の情報セキュリティ対策

情報セキュリティ対策として、まず社員が利用するパソコンやサーバーの対策のみ行い、NAS は後回しにされるケースが多いと思われます。しかしながら情報セキュリティ対策で守るべきは「データ」になります。その重要なデータが保存されている NAS の対策を後回しにすることできません。一方で企業においては「管理者不在」、「コストがかけられない」という課題があります。そこでアイ・オー・データ機器は LAN DISK H を活用した情報セキュリティ対策をご提案いたします。

3. LAN DISK H シリーズの情報セキュリティ対策

LAN DISK H シリーズの情報セキュリティ対策について説明します。まず、情報セキュリティ対策の押さえるべきポイントと LAN DISK H シリーズの機能の関連について説明し、ついで「証拠保全」の要素について解説します。最後に証拠保全に役に立つ LAN DISK H シリーズの「ログ拡張パッケージ」について説明します。

3.1 情報セキュリティ対策の押さえるべきポイント

重要なデータが保存される NAS ですが、運用で押さえるべきポイントを絞りこむことにより、コストを掛けずに導入することが可能です。このポイントは、**「脅威そのものへの対策」**および、万が一事故が発生した際の**「復旧手段の準備」**、発生後に何があったか確認するための**「証拠保全」**の 3 つになります。3 つに分ける理由は、それぞれの対策方法が異なるためです。

「脅威に対する対策」は企業が自発的かつ継続的に実施すべきもので、社員ひとりひとりに関わるものです。**「復旧手段の準備」**は IT インフラ導入時の要件かつ保守運用に関するもので、機器選定者により検討されるべきものです。**「証拠保全」**は万が一のセキュリティインシデント発生時に何が起きたのかを明らかにするためにログを

確実に保全する仕組みで、企業の内部統制に従って管理者が配慮すべきものです。以下に、各ポイントと LAN DISK H シリーズの機能をまとめました。

■ 情報セキュリティ対策マトリクス

ポイント	LAN DISK H シリーズの機能	コスト	関連資料
脅威に対する対策	・ ユーザー登録・グループ登録 ・ 共有フォルダーのアクセス制御	標準機能に含む	**マイナンバー制度に効果的な NAS 運用** http://www.iodata.co.jp/biz/whitepaper/pdf/landiskh_mynumber.pdf
	ファームウェア自動アップデートで常に最新版を適用	標準機能に含む	
	ウイルス対策でファイルをリアルタイム監視	標準機能に含む※	
	内蔵ボリュームの暗号化	標準機能に含む	
	外付け USB ハードディスクの暗号化	標準機能に含む	
復旧手段の準備	外付け USB ハードディスクへの 履歴差分バックアップ	外付け USB ハードディスクなど	**バックアップから始めるセキュリティ** **～ランサムウェア対策のご提案～** http://www.iodata.co.jp/biz/whitepaper/pdf/landiskh_security.pdf
証拠保全	ログ拡張パッケージ	（無償）パッケージ追加で実現	**今回のホワイトペーパー**

※ HDL2-H/TM シリーズ（TMNAS セット品）のみ。

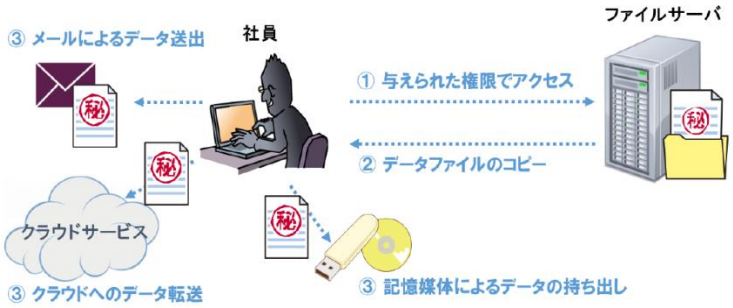
上記より以下のことが分かります。

1. LAN DISK H を利用することにより、コストを掛けずに NAS の情報セキュリティ対策が可能
2. 各種法令の要件についても、標準機能で一部実現可能
3. セキュリティインシデントが発生した場合の、復旧手段と証拠保全も可能

また、ルータ、パソコン、サーバー、NAS それぞれに情報セキュリティ対策を実施することにより、重要なデータを守るための**「多層防御」**を実現することが可能です。

3.2 証拠保全について

証拠保全は、万が一情報漏えい等のセキュリティインシデントが発生した際の調査や証拠として活用することを目的に操作ログやシステムログなどの情報を確保しておくことを言います。このとき役に立つのが NAS の「アクセスログ」です。アクセスログは全てのファイル操作を記録することから、抑止力として内部不正対策にも有効です。（内部不正とは正規の権限を持つ内部者が、外部に情報を漏らす行為です。）



＜引用＞IPA「企業における情報システムのログ管理に関する実態調査」報告書

https://www.ipa.go.jp/security/fy28/reports/log_kanri/

NAS のアクセスログが内部不正に有効な理由は以下のとおりです。

1. 不正行為を行った内部者（社員等）を特定することができる
2. 情報漏えい等の証拠となるアクセスログを確保することができる
3. 従業員に対しアクセスログの取得を通知することで不正行為を抑止する

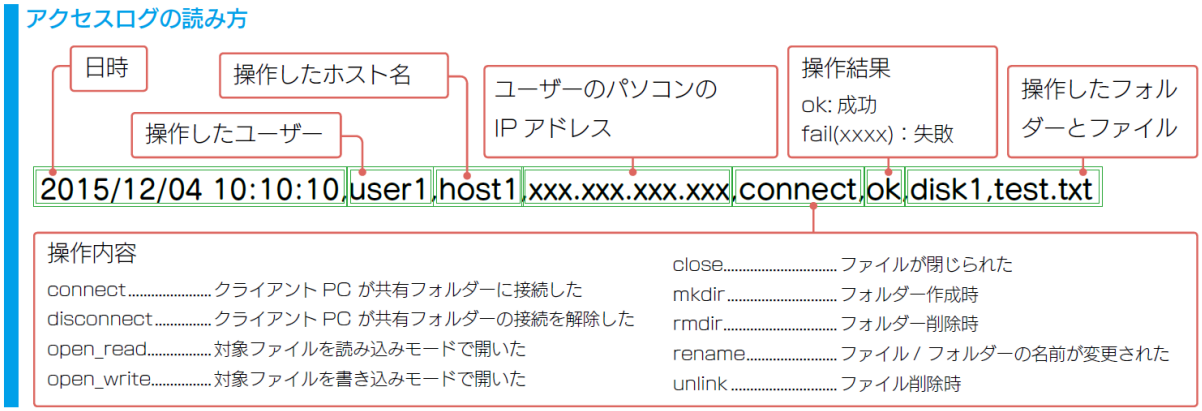
3.3 ログ拡張パッケージ

LAN DISK H シリーズでは、証拠保全を行う追加機能の提供を 2016 年 1 月より開始しました。その機能が「ログ拡張パッケージ」です。この「ログ拡張パッケージ」を利用することにより、証拠保全に役立つ機能を LAN DISK H シリーズで利用することが可能になりました。

＜参照＞情報漏えいリスクから会社を守る！セキュリティ機能搭載ビジネス NAS

http://www.iodata.co.jp/ssp/nas/w_security/index.htm

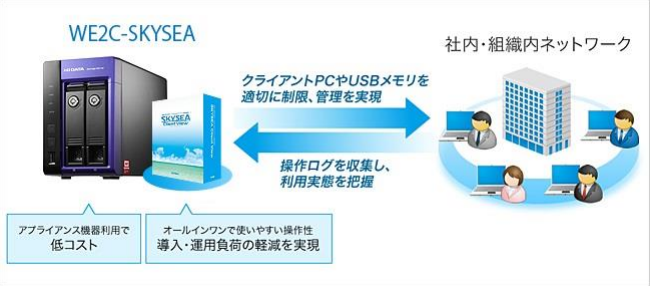
【ログ拡張で取得可能な内容】



【パソコンの操作ログ取得について】

「ログ拡張パッケージ」は、NAS へのファイル操作に対するログを記録します。パソコン内部で処理されたファイル操作については記録できません。

パソコンの操作ログを保全する仕組みとしては、情報漏えい対策・IT 運用管理ソフトウェア「SKYSEA Client View」を搭載したパッケージモデル WE2C-SKYSEA をご提案します。「WE2C-SKYSEA」と「ログ拡張パッケージ」を併用することにより、クライアント PC と NAS 双方の効果的な情報セキュリティ対策を行うことが可能です。



※ 管理するデバイスの最大数は 20 台まで対応。

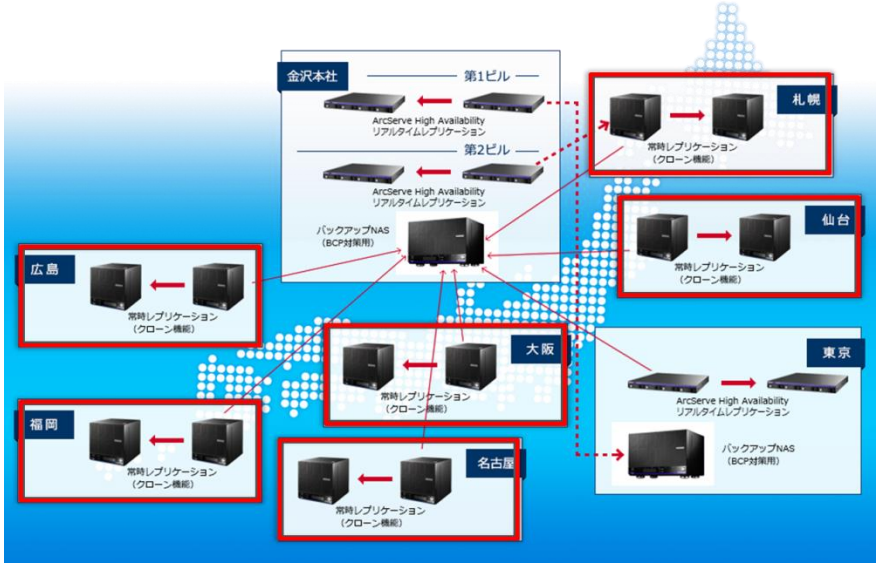
※ SKYSEA Client View ソフトウェアはインストール済み。ソフトウェアライセンスを別途、Ｓｋｙ株式会社販売代理店より購入が必要

4.「ログ拡張パッケージ」の実導入事例

本章および次章では、実際の運用環境で LAN DISK H シリーズの「ログ拡張パッケージ」を利用した事例をご紹介いたします。これはアイ・オー社内のファイルサーバーで 3 ヶ月間運用した事例となります。本章では、当社のファイルサーバーの運用環境を紹介し、測定ツールと役割について説明します。最後に実際の設定例をご紹介します。

4.1 アイ・オー自社のファイルサーバー運用

アイ・オーでは Windows Server 2003 サポート終了に伴い、企業内共有ファイルサーバーに代わり自社商品 LAN DISK Z シリーズならびに LAN DISK H シリーズを導入しました。今回、全国６拠点に設置された LAN DISK H シリーズに「ログ拡張パッケージ」を追加して、アクセスログを取得しました。



＜参照＞導入事例：【アイ・オー】自社ファイルサーバーを NAS へリプレイス

http://www.iodata.co.jp/biz/ws2003/io2003eos/index.htm

計測を行った拠点は以下のとおりです。

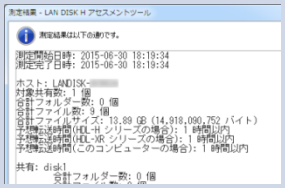
1. 札幌営業所
2. 仙台営業所
3. 名古屋営業所
4. 大阪営業所
5. 広島営業所
6. 福岡営業所

今回の取得目的は以下のとおりです。

- 各拠点の LAN DISK H シリーズの活用状況の確認。
- アクセスログの増加状況および、増加条件の確認
- 業務でのアクセスログ利用の実態の確認

4.2 計測ツールと役割

取得目的に応じて、二種類の計測ツールを利用して情報収集を行いました。以下に表で示します。

取得目的	利用ツール	集計方法	備考
NAS の利用状況	アセスメントツール（Windows アプリ） 	測定結果より集計 	LAN DISK H アセスメントツール http://www.iodata.co.jp/product/app/nas/landickh_assessmenttools/index.htm
アクセスログの状況	LAN DISK H 「ログ拡張パッケージ」 	保存された CSV ファイルより、増加容量を手動でカウントし、集計。 	LAN DISK H シリーズのパッケージ追加（機能追加） http://www.iodata.co.jp/product/nas/info/landisk/hdl-h_package.htm

4.3 実際の設定例

今回の設定は、最初に「ログ拡張パッケージ」の追加を行い、次に基本設定を行いました。最後にアラート設定を行っております。

①「ログ拡張パッケージ」を追加する

ログ拡張パッケージを追加します。

[システム] → [パッケージ管理] → [追加] をクリックします。

① [ログ拡張パッケージ]をチェックします。
② [追加]をクリックします。

②「ログ拡張」を設定する（抜粋）

次にログ拡張の設定を行います。

[ログ拡張] → [設定] をクリックします。

① ［アクセスログを取得する共有フォルダー］では、ファイルとして記録するアクセスログの対象フォルダーを選択します。
② [アクセスログファイルを自動的に削除する]を有効にし、削除条件を設定します。

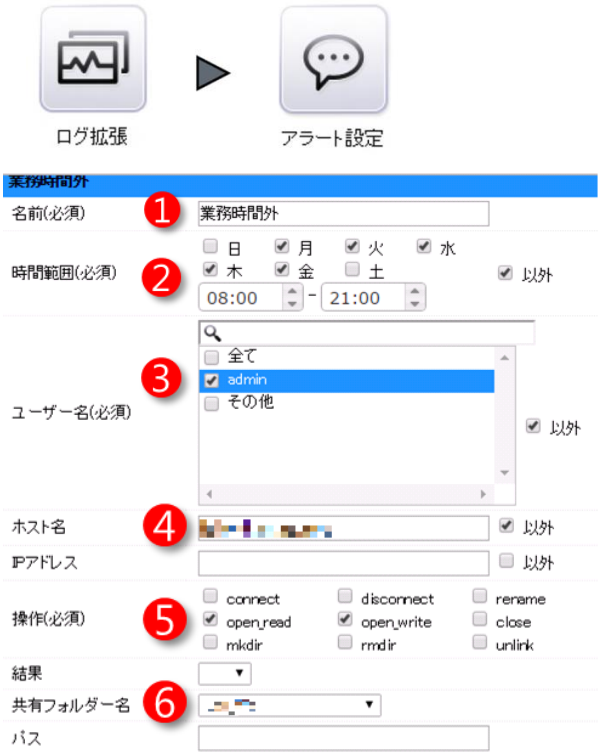
ここでのポイントは以下のとおりです。

1. 実際に運用している共有フォルダーを指定することにより、アクセスログの容量を節約することができます。
   例１）指定するフォルダー：個人情報を保存している共有フォルダーなど
   例２）指定しないフォルダー：クライアントのバックアップを保存している共有フォルダーなど
2. 自動削除設定することにより、アクセスログによる共有フォルダーの容量圧迫を防ぎます。
   アクセスログの容量目安は次章を参照下さい。

⚠ 内蔵ボリュームの容量が不足すると、アクセスログ記録が中止されます。そのため、古いアクセスログファイルを自動削除するよう設定されることをオススメいたします。また自動削除設定時かつ全てのログファイルを保存しておきたい場合は、定期的に取りだして他のストレージへ保存されるよう運用してください。

③ 業務時間外のアラート設定例

最後にアラートログの設定を行います。ここでは業務時間外（平日の 21:00 から翌日 8:00 まで）の管理者以外のアクセス（ただし、バックアップを除く）に対してアラートを行う設定をします。



[ログ拡張] → [アラート設定] をクリックします。

① [名前（必須）]任意のアラート名を入力します。
② [時間範囲（必須）]対象の曜日と時刻範囲を指定します。
③ [ユーザー（必須）]対象のユーザー名を設定します。
④ [ホスト名]対象のホスト名を設定します。
⑤ [操作（必須）]対象となる操作を選択します。
⑥ [共有フォルダー名]対象となる共有フォルダー名を選択します。

※ 上記設定で[以外]にチェックをつけると設定範囲および内容以外が対象となります。

ここでの設定ポイントは以下のとおりです。

設定ポイント	入力箇所	入力方法
業務時間外の指定	時間範囲（必須）	実際の業務時間を指定（平日の 8:00 – 21:00）し、[以外]にチェックする
バックアップ時のアクセスログ除外	ホスト名	ホスト名にバックアップ先の PC 名を入力し、[以外]をチェックする ・ バックアップがネットワーク上の共有フォルダーの際有効
アラートログの削減	操作（必須）	操作項目の絞込

以上で、設定完了です。

5. 実行結果

上記の設定を行い、3ヶ月にわたり全国 6 拠点の NAS の定点観測を実施しました。

観測期間：　2016 年 2 月から 5 月の 3ヶ月間

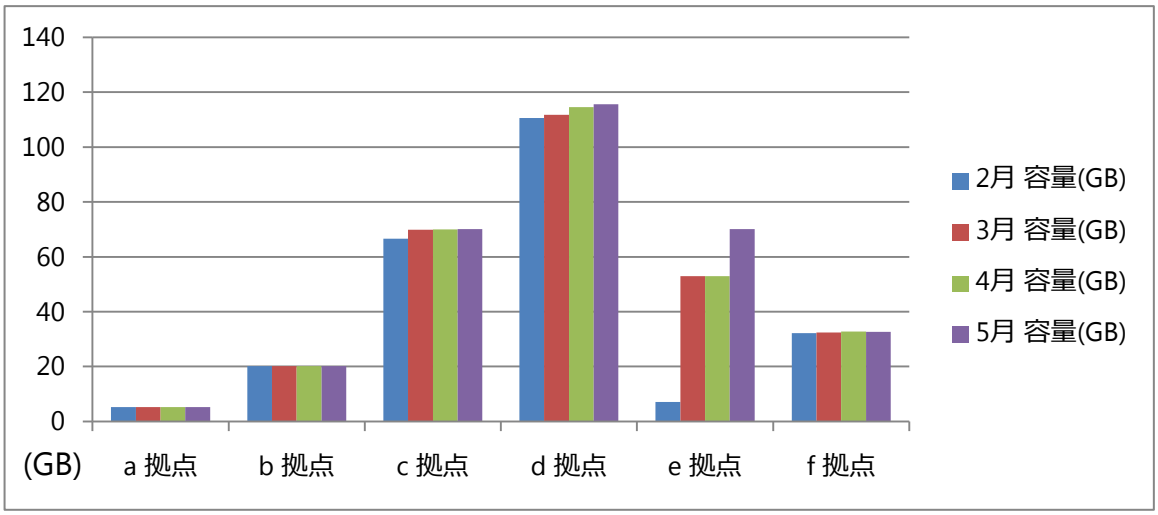
観測ポイント：　札幌、仙台、名古屋、大阪、広島、福岡の 6 営業所

※ 以下の実行結果データでは、拠点名は a 拠点、b 拠点、c 拠点・・・と表記します。

観測目的：

- 各拠点の LAN DISK H の活用状況の確認。
- アクセスログの増加状況および、増加条件の確認
- 業務時間外の NAS の利用状況の確認

5.1 各拠点の LAN DISK H の活用状況

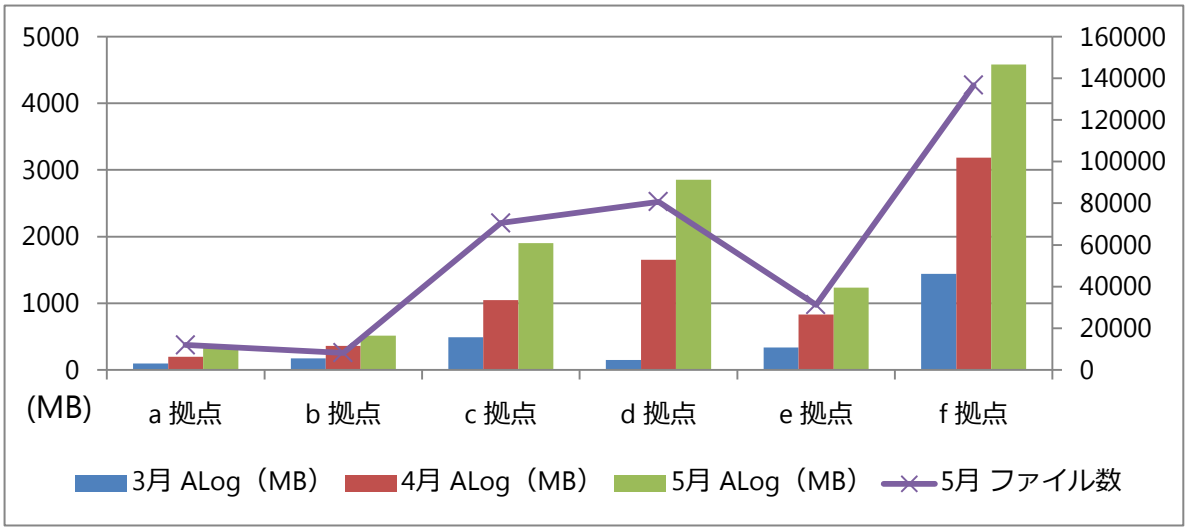


各拠点の NAS のディスク利用状況は拠点規模および、拠点の NAS の利用方法により大きく異なります。

これらの情報から各拠点の運用特性が見えてきました。

1 ファイルあたりの容量	特徴
500KB 未満	Excel 等の業務データが多い
500KB 以上、2M 未満	PowerPoint の提案書および、写真データが多い
2M 以上	・ PowerPoint の提案書および、写真データが多い ・ バックアップデータを含む

5.2 アクセスログの増加状況および、増加条件



上記グラフからアクセスログの 2 つの特性が読み取れます。

1. アクセスログの増加は拠点のファイル数に依存する
2. アクセスログは毎月等倍に増加する。

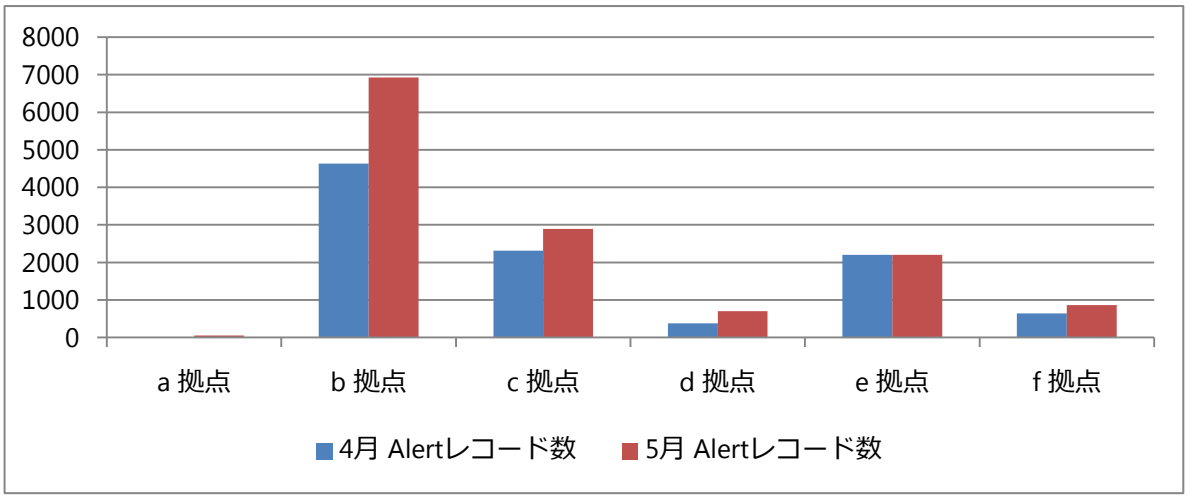
このことから、業務形態や人員構成が変わらない場合、アクセスログは一定の増加が見込まれます。

現状の数値推移からアクセスログ増加のシミュレーションを行いました。

ファイル数	ファイル数目安	アクセスログ目安※				
		1 月	6 ヶ月	1 年	3 年	5 年
多い	100,000	1.5 GB	9.0 GB	18.0 GB	54.0 GB	90.0 GB
普通	50,000	0.5 GB	3.0 GB	6.0 GB	18.0 GB	30.0 GB
少ない	10,000	0.1 GB	0.6 GB	1.2 GB	3.6 GB	6.0 GB

※ 運用中のファイル増加および、突発的なファイル増加は含めておりません。また、数値は目安です。

5.3 業務時間外の NAS の利用状況



アラートログの結果から、以下のことがわかりました。

- b拠点は所長が早朝出勤していることが、アラートログから判明した。NASのアラートブザーに気がついた所長より連絡があり、早朝の時間外設定を変更した。
- 他の拠点は 21:00 以降のアクセスが多いことから、残業の課題が見えてきた。

アクセスログは、万が一情報漏えい等のセキュリティインシデント時の証拠保全だけでなく、通常業務のちょっとした変化に対する事実確認としても活用できます。アクセスログは、NAS の運用の変化をとらえた際、発生している事象を確認するために、非常に有益な情報で、詳細に見ていくことにより、後から「誰が」「いつ」「どのファイルに対して」「何をしたか」とうい事実を明らかにすることが可能です。

6. 最後に

企業のセキュリティ対策状況を調査したデータ※によると、「ログ情報の統合・分析、システムのセキュリティ状態の総合的な管理機能」を導入していたのは、大企業でも 29.9%であったのに対し、中小企業は 7%でした。

LAN DISK H の「ログ拡張機能」は、投資金額が限られている場合でも、コストを掛けることなく証拠保全に役立つ機能をご提供いたします。さらに LAN DISK H は、証拠保全だけでなく、有益な情報セキュリティ対策の機能を用意しています。

本ホワイトペーパーでは LAN DISK H のセキュリティ機能を中心に説明させていただきました。NAS はファイルサーバー機能を中心に利用される装置ですが、機能を有効に活用することで情報セキュリティ対策にご利用いただくことも可能です。是非ご活用いただければと思います。

※ ＜参照＞IPA「中小企業における情報セキュリティ対策に関する実態調査」
http://www.ipa.go.jp/security/fy27/reports/sme/index.html