進化する明日へ Continue thinking
I-O DATA

ホワイトペーパーシリーズ：

マイナンバー制度に効果的な NAS 運用

セキュリティを意識した LAN DISK H の運用方法

2015 年 5 月

内容

1. 概要

1.1 このホワイトペーパーについて

「行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、マイナンバー法）」が施行され、平成 27 年 10 月以降、日本国内の全住民にマイナンバーが通知されます。多くの企業でこのマイナンバー法に基づくマイナンバー制度について検討されていると思います。
マイナンバー制度対応のためのシステム改修の第一歩は、人事・会計ソフトのバージョンアップからですが、マイナンバーを取り扱う全ての事業者には安全な管理体制、つまり全従業員のマイナンバー情報を収集し、しっかりと管理し、漏らさないような運用を求められます。
本ホワイトペーパーでは、小規模企業のマイナンバー制度対策、特にセキュリティ強化を考慮し、安全に NAS を運用する方法についてご紹介いたします。

1.2 マイナンバー制度のポイント

日本国内の全住民にマイナンバー（12 桁の個人番号）が割り当てられ、平成 28 年 1 月から社会保障・税・災害対策に限定し、行政手続きで使用がはじまります。

マイナンバー制度の詳細については、以下の URL を参照ください。

■ 内閣官房 WEB ページ：マイナンバー社会保障・税番号制度
http://www.cas.go.jp/jp/seisaku/bangoseido/

それに伴い、全ての事業者も、税や社会保険の手続きで、従業員などのマイナンバーを取り扱うこととなります。
マイナンバーを取り扱う際に、すべての事業者が気をつけなくてはならないポイントは以下のとおりです。

1. **厳しい罰則規定**
   個人に配布される、マイナンバーの変更は原則できません。そのため、万一漏れてしまうと未来永劫に渡って情報が公開されてしまうこととなり、事業者に対しては罰則規定を重くして、厳重な管理を行うよう求められています。
2. **安全管理措置が義務付けられる**
   マイナンバーを取り扱うために、安全な管理体制が求められています。
   特にマイナンバーをその内容に含む個人情報である「**特定個人情報**」の取扱には細心の注意を求められています。
3. **ガイドラインが提示されている**
   マイナンバーの取り扱いについて法律が求める保護措置およびその解釈について、具体例を用いて説明するために「特定個人情報の適正な取扱に関するガイドライン（事業者編）」が示されています。

上記、ガイドラインの適用については中小規模事業者に対する特例を設けることにより、実務への影響に配慮しています。しかしながら、マイナンバー制度は法律で定められた制度のため、会社規模を問わず、求められる内容や罰則規定は同様となります。つまり、「中小規模事業者なので、マイナンバー対策をしなくてよい」ということはありません。逆にこれまで個人情報保護法の適用がなく、個人情報取扱のための安全管理措置が取られていない中小規模事業者の場合、しっかりとした運用体制を準備する必要があります。

1.3 安全管理措置について

ガイドラインには安全管理措置の考え方が記載されています。このガイドラインは組織の仕組みづくりも含んだガイドラインとなっており、機器購入のためのガイドラインではありません。安全管理措置は以下のとおりです。

*出展：«ここがポイント»マイナンバーガイドライン（特定個人情報保護委員会事務局）より作成
http://www.ppc.go.jp/files/pdf/270213shacho.pdf

企業規模や組織体制、さらに業種業態により、安全管理措置の取り組み方が異なるため、事業者によって安全管理措置の取り組みポイントが異なります。以下に事例を示します。

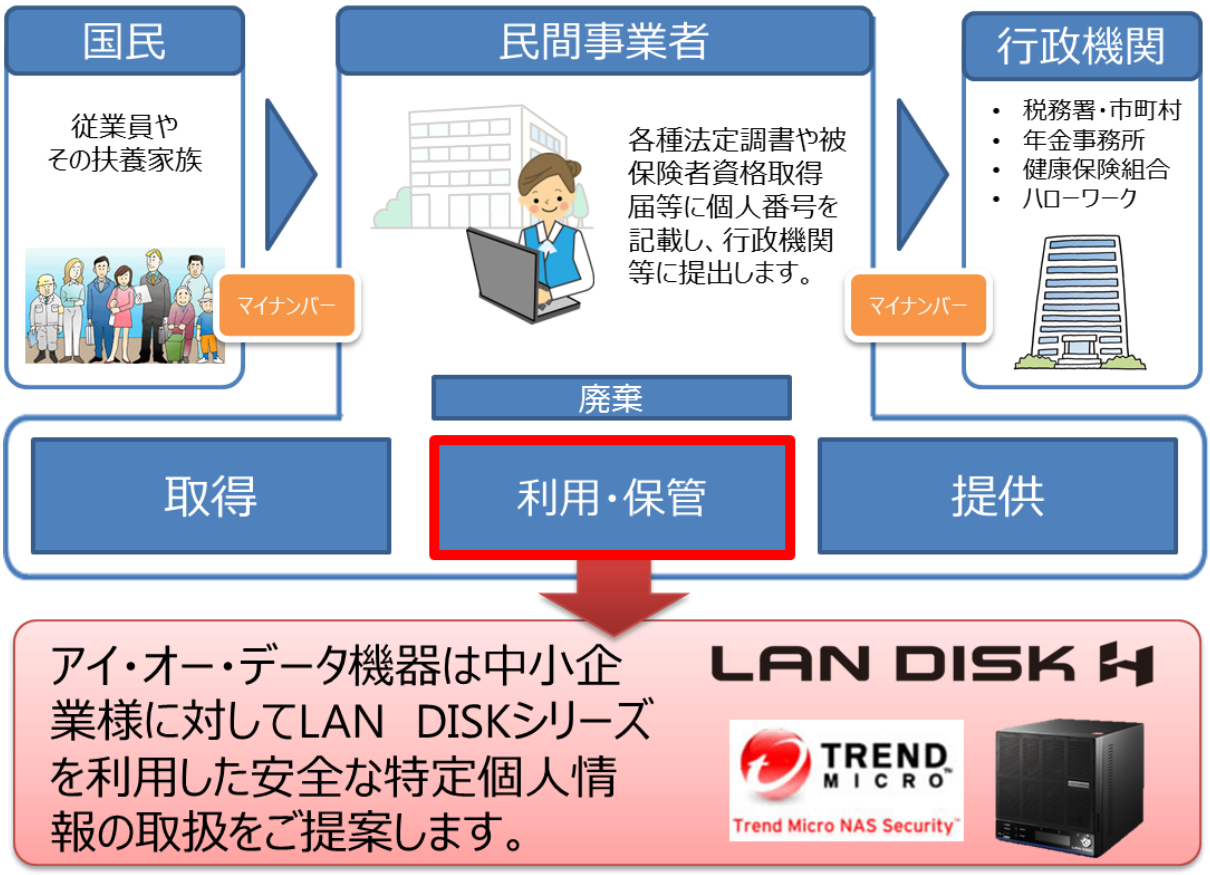
	1.機械加工メーカー	2.外食産業	3.情報機器メーカー
社員数	社員数：18 名	社員：120 名 パート･アルバイト：300 名	社員数：500 名
拠点数	本社 1 箇所	店舗：150 箇所	本社 1 箇所。拠点 8 箇所
個人情報取扱	なし	あり	あり
マイナンバー対策の課題	マイナンバー情報の取扱方法	店舗からの個人情報の収集方法	廃棄スキームの構築
備考	個人情報取扱は初めてのため、何から実施してよいかわからない。社員の顔が見えるから収集はなんとかなると思うが･･･	顧客情報収集のため、個人情報取扱の仕組みはあるが、出入りが激しいパート･アルバイトの情報をどう集めるかが課題	ユーザー登録情報の収集の経験があり、個人情報取扱の仕組みはある。収集は紙で行い、本社で特定個人情報ファイル化を行う。

上記例の通り、各事業者により課題が異なります。そのため、各事業者にあった安全管理措置を検討する必要があります。つまり、マイナンバー対策のために何か一つ購入すれば大丈夫ということはなく、事業形態に合わせた、運用を含めた考慮が必要となります。

今回、アイ･オー･データ機器は「１． 機械加工メーカー」を例とする、中小規模の事業者を対象として、マイナンバー保管の課題に対して LAN DISK H を提案いたします。

1.4 LAN DISK H のご提案

マイナンバー対策は単一の商材で全てをカバーすることはできませんが、自社の現状を把握することによりポイントを押さえた対応を行うことが可能です。



*出展：マイナンバーガイドライン入門（特定個人情報保護委員会事務局）より作成
http://www.ppc.go.jp/files/pdf/270213guideline.pdf

企業に求められる安全管理措置に対して、LAN DISK H がカバーする内容は以下のとおりです。

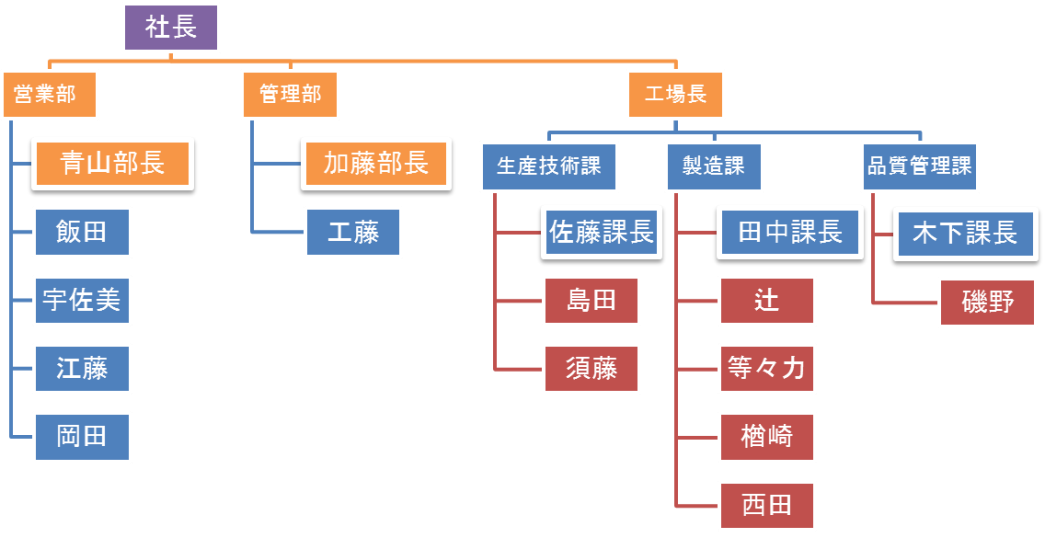
安全管理措置	対策	LAN DISK H の機能
組織的安全管理措置	アクセスログ取得	共有フォルダーのアクセスログ機能
技術的安全管理措置	ユーザー登録、グループ登録	ユーザー登録・グループ登録
	共有フォルダーのアクセス制御	共有フォルダーのアクセス制御
	OS の脆弱性対策	ファームウェア自動アップデートで常に最新版を適用
	ウイルス感染による不正アクセス対策	（有償オプション）TMNAS Security でファイルをリアルタイム監視
	情報漏えいからの保護	内蔵ボリュームの暗号化
		外付け USB ハードディスクの暗号化

本ホワイトペーパーではこの安全管理措置に適用した、セキュリティを意識した LAN DISK H の運用方法を紹介いたします。

2. 機械加工メーカーの想定導入ケース

2.1 今回の想定利用シーン

- 業種：機械加工メーカー
- 従業員数： １８名
- 所有 PC 台数： ２５台（業務用、作業管理用含む）
- 拠点：本社一箇所
- 現状：
  - 取引先からの機械加工受注が事業の柱
  - 個人と直接やり取りがないため、個人情報取扱の準備はされてない
  - 事務系、生産系の IT システムはそれぞれパッケージソフトを利用（一部カスタマイズあり）
  - 老朽化したサーバーを利用しており、パッケージソフトのバージョンアップと併せて入れ替えを検討している。
- 組織図



- マイナンバー対策
  - マイナンバーの対策は管理部主導で実施
  - 組織としての基本方針や取扱規程取りまとめはほぼ完了し、課題に対する対応を検討中
  - 特定個人情報取扱担当者は以下のとおり
    - 代表者：社長
    - 責任者：管理部　加藤部長
    - 取扱担当者：管理部　工藤

    ※ 管理部　加藤部長は情報システムの責任者も兼任する。
  - 人事・給与のマイナンバー対応はパッケージソフトのアップグレードで対応予定
  - 社員数が少なく、顔が見えるため、マイナンバー収集は直接本人から紙ベースで取得する
  - 取得したマイナンバーは、特定個人情報取扱担当者が電子ファイル化（特定個人情報ファイル）して利用・保存・提供を行う。電子ファイル化する理由は業務の効率化と人の入れ替わりの際のメンテナンス性を良くするため。

■ 予算
- パッケージソフトのアップグレードは予算化済み
- セキュリティ対応も予算化済みだが、購入製品は検討中

■ 課題
- セキュリティ対応としてどこから行えばよいのか分からない
- 収集したマイナンバーを含む特定個人情報をどのように保管すればよいか迷っている
- マイナンバー専用機器は予算の都合から導入が難しい

2.2 セキュリティを意識した LAN DISK H の運用方法

今回のユーザー課題に対して、LAN DISK H をご提案いたします。
LAN DISK H を利用することにより限られた予算の中で、以下のように安全管理措置を満たした運用することが可能です。

LAN DISK H
TREND MICRO
Trend Micro NAS Security™

1）組織的安全管理措置：取扱規程に基づく運用が可能

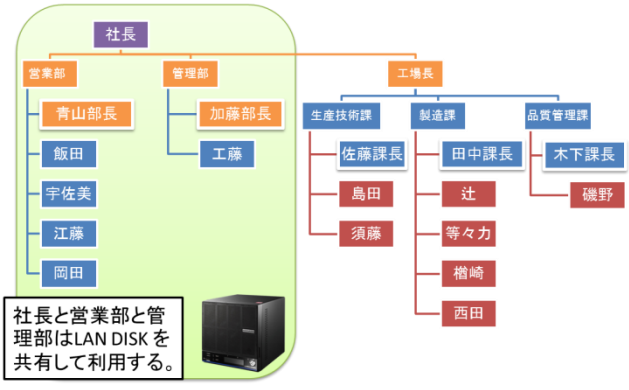
LAN DISK H のアクセスログ機能を利用することにより、運用状況確認のために、共有フォルダーへのアクセスを記録することができます。
このアクセスログ機能は、誰がいつファイルの参照・作成・編集を行ったかなどのアクセス記録がリアルタイムに記録されます。また、管理者宛にメールでログを一括転送するように設定できますので、監査記録として利用することができます。

⚠ 本機能は Microsoft ネットワーク共有で共有フォルダーへアクセスした場合のみご利用いただけます。パッケージ追加で利用可能な AppleShare ネットワーク共有、FTP 等のアクセスログは記録されません

2）技術的安全管理措置：アクセス制御、アクセス者の識別と認証が可能

適切なアクセス制御を行うことにより、特定個人情報にアクセスする範囲を限定することが可能です。
今回の事例では安全管理措置の取扱規程等の策定および、組織的安全管理措置より、NAS の共有フォルダーの技術的安全管理措置のアクセス制御を以下の通り行います。

1．特定個人情報ファイル保存利用と業務利用の兼用
※緑の枠の範囲で LAN DISK H を利用。
LAN DISK H のセキュリティ運用を業務全体に適用することにより、全社のセキュリティ運用を高める効果を期待しています。



2．共有フォルダー及びアクセス権の設定
設定した運用に従い、共有フォルダーと社員のアクセス権を設定
(ア) 特定個人情報は「個人情報」の共有フォルダーに格納（赤枠）
隠し共有とし、不要な人が不要な情報にアクセスしない仕組みを強化する。
(イ) 個人別のバックアップフォルダーを作成し、定期的なバックアップ環境を提供する。

(ウ) 全ての共有フォルダーはゲストユーザからのアクセスを禁止し、厳密なアクセス運用を徹底する。

⚠ 個人別のバックアップフォルダーは使用量制限することをオススメいたします。これは複数のクライアント PC のバックアップデータを NAS に複数世代保存すると、NAS の容量を圧迫するためです。

⚠ クライアント PC のバックアップ運用は以下の運用をご検討ください。詳細はご利用のバックアップソフトの詳細をご確認ください。

- ✧ 世代数を制限する
- ✧ バックアップソフトの圧縮機能を有効にする

■共有フォルダー及びアクセス権の設定マトリクス

ルート	共有フォルダー名	備考	社長	営業部					管理部	
				青山部長	飯田	宇佐美	江藤	岡田	加藤部長	工藤
	個人情報	共有	R/W	×	×	×	×	×	R/W	R/W
	管理職		R/W	R/W	×	×	×	×	R/W	×
	営業部		R/W	R/W	R/W	R/W	R/W	R/W	R/W	×
	管理部		R/W	×	×	×	×	×	R/W	R/W
	社長	バックアップ（100G制限）	R/W	×	×	×	×	×	R/W	×
	青山		×	R/W	×	×	×	×	R/W	×
	飯田		×	R/W	R/W	×	×	×	R/W	×
	宇佐美		×	R/W	×	R/W	×	×	R/W	×
	江藤		×	R/W	×	×	R/W	×	R/W	×
	岡田		×	R/W	×	×	×	R/W	R/W	×
	加藤		×	×	×	×	×	×	R/W	R/W
	工藤		×	×	×	×	×	×	R/W	R/W

3）技術的安全管理措置：外部からの不正アクセス等の防止が可能

1. LAN DISK H にはファームウェアの自動更新機能がついており、常に最新の状態でご利用いただくことが可能です。ファームウェアの更新（アップデート）には、新しい機能の追加のほかにも本製品の修正など、重要な更新が含まれます。ファームウェアの自動更新機能を有効に設定しておくことをおすすめします。（出荷時設定：有効）
2. TMNAS Security（以下、TMNAS）が LAN DISK H の共有フォルダーに書き込まれたファイルがウイルスに感染していないかをリアルタイムで監視しています。万が一ウイルス対策の不十分なパソコンをネットワークに接続し、ウイルス感染したファイルを LAN DISK の共有フォルダーに転送した場合も、NAS 自身が保存されたウイルス感染ファイルを駆除・隔離します。

4）技術的安全管理措置：情報漏えい等の防止が可能

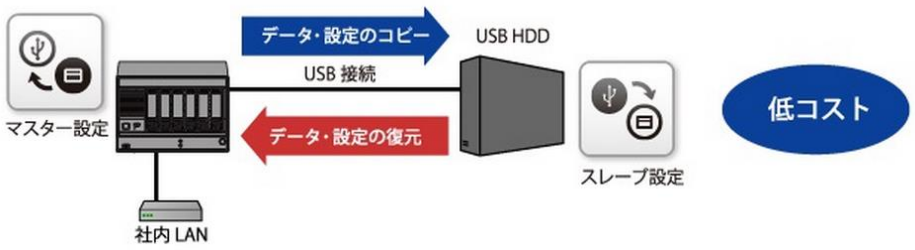
LAN DISK H 情報漏洩対策として、万一盗難に遭っても情報が漏れないようディスク全体を暗号化します。LAN DISK H の暗号化ボリューム機能は、本製品の内蔵ディスク、専用フォーマットの外付け USB ハードディスクを丸ごと暗号化する機能です。

暗号化機能を有効にすると、起動時に専用の鍵(USB ロックキー) をつながない限り、暗号化されたディスク領域にアクセスすることはできませんので、万一本製品を丸ごと、あるいはハードディスクカートリッジの盗難に

あった場合でも、記録された情報の漏洩を防ぐことができます。暗号化には高度な AES 方式（256bit）を用いており、安全に処理されます。

今回は LAN DISK H のクローン機能のうち『システム保存設定』を使って外付け USB ハードディスクにバックアップします。本機能を利用することにより、データは履歴差分バックアップ機能により保存され、さらに LAN DISK H の設定情報も暗号化して保存されます。
万一 LAN DISK H シリーズに障害が発生したときは、新しい LAN DISK H シリーズにクローン先の USB ハードディスクを接続し、データと設定情報の復元を行うことにより復旧します。データを復元するのに容量に応じた時間が掛かりますが、設定情報の復元も手間無く行うことができ、低コストで備えることが可能です。

■クローン機能を利用した USB ハードディスク バックアップ



本機能の詳細と導入手順は以下のホワイトペーパーを参照ください。

■LAN DISK H シリーズ クローン機能の紹介
http://www.iodata.jp/solutions/whitepaper/12dh9400001xpvkr-att/hdi-h_clone.pdf

2.3 LAN DISK H の導入

1. 商品選定理由

今回、HDL2-H4/TM5 を選定しました。容量はクライアントバックアップ領域が社長を含め 8 名：800GB 必要なため、将来の拡張性も考慮して実用量 2TB の HDL2-H4/TM5 とします。同時にバックアップ HDD を含め以下の構成で購入しました。（2TB x 2 ドライブ、拡張ボリューム運用で 2TB）としました。

製品		定価（税別）	備考
HDL2-H4/TM5		¥135,000	Trend Micro NAS Security 搭載モデル ライセンス期間 5 年版 4TB（実用量 2TB）
ISS-LGL-PR5		¥176,000	HDL2-H4/TM5：オンサイト保守パック 5 年版
ZHD-UTX3		¥46,800	バックアップ用カートリッジ式外付け USB HDD。3 年保証 3TB
ISS-LHA-PR5		¥77,000	ZHD-UTX3：オンサイト保守パック 5 年版
UPS（社外品）		¥23,800	＜参考＞オムロン社 BY35S の場合
SDS_NCL-665（取扱商品）		OP 価格（¥50,000）	小型 19 インチラック W600×H600×D550 （11U）35kg
	合計	¥508,600	※ 全て定価もしくは想定売価の合計。 ※ 消費税は除く

2. LAN DISK 設定手順

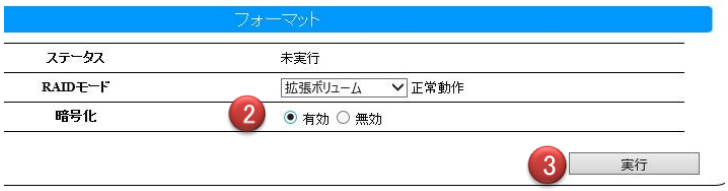
今回機能設定は以下の順序で実施します。

設定順序	設定内容	LAN DISK H の機能
1	内蔵ディスクの暗号化ボリューム作成	暗号化設定
2	外付け USB HDD の暗号化	
3	自動アップデート機能の確認	ファームウェア自動アップデート
4	アクセスログ機能の設定	Windows 共有機能のアクセスログ
5	TM パッケージのアクティベーション	TMNAS Security の有効化
6	一括登録の実施	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
7	クローンバックアップの実施	システム保存設定

2.4 実際の手順

手順 1 ：内蔵ディスクの暗号化ボリューム作成

暗号化ボリュームを作成するには［ボリューム］→［内蔵］→［フォーマット］をクリックしてください。



① 上図 製品本体添付の USB メモリーを本製品全面の USB ポート 1 につなぐ
② [暗号化] の[有効]を選ぶ
③ [実行]をクリック

⚠ 暗号化に利用するキーは USB ロックキー内にのみ存在します。万一 USB ロックキーが壊れたり、紛失した場合、暗号化ボリュームにアクセスできなくなります。必ず「マスターキー」と「スペアーキー」の複数の USB ロックキーを用意し、万一に備えて「マスターキー」を安全な場所に保管しておいてください。

⚠ スペアーキーの作り方は、LAN DISK H シリーズの画面で見るマニュアルを参照ください。

⚠ 起動時に USB ロックキーを接続して暗号化されたボリュームを接続したら、USB ロックキーを取り外し安全な場所に保管してください。装置とともに USB ロックキーが盗難に遭うと情報漏えいにつながります。

手順２：外付け USB ハードディスクの暗号化

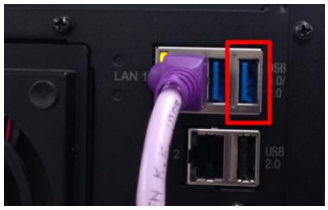
外付 USB ハードディスクも専用フォーマット時に暗号化機能を有効に設定することで書き込み時に自動的に暗号化することができます。

手順２－１：USB ハードディスクを USB4 ポートに接続する

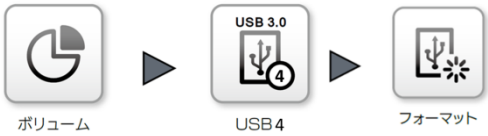
USB ハードディスクを LAN DISK H の USB ポート４に接続

※ USB 右図赤枠が USB ポート４（USB3.0 対応）

※ 今回は、バックアップでクローン機能を利用するため、クローン機能専用の USB ポート４に接続して利用します。



手順２－２：USB ハードディスクの暗号化フォーマットを行う



［ボリューム］→［USB4］→［フォーマット］をクリックす。

⚠ 暗号化する USB ハードディスクは、本製品専用フォーマットにする必要があります。

手順３：自動アップデート機能の確認

手順３－１：ファームウェアの自動更新を確認する

ファームウェアの自動更新（アップデート）は、以下の画面から設定確認いただけます。

※出荷時設定では、ファームウェアの自動更新は有効に設定されています。

［システム］→［ファームウェア］→［自動更新設定］をクリック

① ［自動更新］が有効になっていることを確認する。

② ［時刻］を確認する。

③ ［適用］をクリック

⚠ 実際の自動更新は設定した時刻から１時間以内に行われます。ファームウェアアップデートにより再起動される場合があるため、再起動が行われてもよい時間を設定ください。

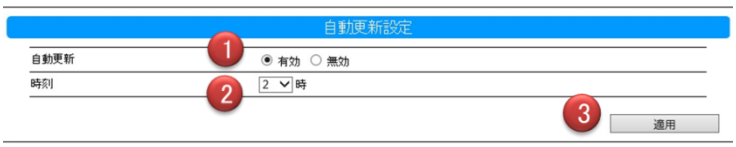
⚠ LAN DISK H がインターネットに接続できない場合は、ファームウェアを弊社ホームページからダウンロードして手動で適用ください。

手順３－２：パッケージの自動更新を確認する

すでに適用したパッケージの更新が見つかった場合に、自動的に更新する設定をおこないます。

※出荷時設定では、有効に設定されています。

［システム］→［パッケージ管理］→［自動更新設定］をクリック



① [自動更新]が有効になっていることを確認する。
② [時刻]を確認する。
③ [適用]をクリック

手順４：アクセスログ機能の設定

手順４－１：アクセスログを有効にする

［サービス］→［一覧］をクリック

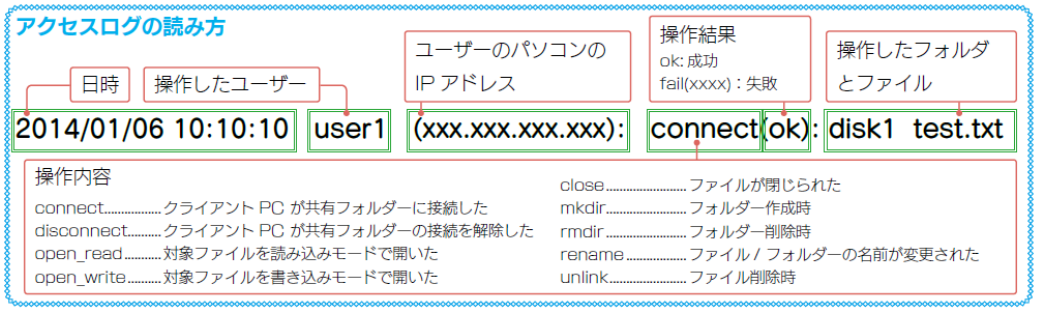
① [アクセスログ]の[有効]を選ぶ
② [適用]をクリック

> ⚠ ログ情報は次のような状況のときに古いログから削除されます。１）ログのサイズが一定のサイズを超えた場合。２）本製品のシャットダウンを 10 回以上行った場合。
> ⚠ アクセスログ情報を定期的に保存するために、自動送信するメール送信機能をお勧めいたします。自動送信のタイミングはアクセするログが一定サイズ追加された場合になります。メール送信する機能は、LAN　DISK H シリーズの画面で見るマニュアルを参照ください。
> ⚠ メール送信をご利用頂く場合、一度に共有フォルダーのアクセスが集中した場合はメールが大量に送信される場合がございます。

手順４－２：アクセスログを確認する

［情報］→［アクセスログ］をクリック
アクセスログが表示されます。

■アクセスログの見方



手順５：TMNAS Security パッケージの適用・アクティベーション

本製品をご利用になる前に、「アクティベート」をしてください。アクティベートを実行することにより、TMNAS の機能が利用可能になります。また、アクティベート、パターンファイルの更新には、LAN DISK H シリーズがインターネットに接続されている必要があります。以下に、初期状態で有効になっている機能を記載します。詳細な設定はマニュアルをご参照ください。

- リアルタイム検索機能
- ウイルスパターンの自動更新機能
- スパイウェア／グレーウェアパターンの自動更新機能
- 検索エンジンの自動更新機能

手順５－１：管理者パスワードの設定

TMNAS 機能を利用する場合、管理者パスワードが必要となります。管理者パスワード設定は［システム］→［管理者設定］をクリックください。

① ［パスワード］および［パスワード（確認）］を入力
② ［適用］をクリックする

⚠ ファームウェア Ver.2.00 以降が適用されている場合、LAN DISK H 初回起動時に４文字以上の管理者パスワード設定が必須となります。登録済の場合は別途設定する必要はありません。

手順５－２：TMNAS 機能のアクティベートを行う。

TMNAS のアクティベートについては以下のマニュアルをご参照ください。
パッケージ取扱説明書「TMNAS Security」
http://www.iodata.jp/lib/manual/pdf2/hdlh-tmnas-manual.pdf

手順６：一括登録の実施

ユーザー・グループ・共有フォルダーのリスト（CSV ファイル）を作成し、本製品に読み込ませると、一括登録をすることができます。この機能を利用すると大人数のユーザー登録や、複雑なアクセス制御を持つ共有フォルダーを一括して登録できます。

手順６－１：一括登録ファイル（CSV ファイル）の作成

今回 CSV 作成のための補助ツール「一括登録テンプレート.CSV」を準備しました。設定詳細は LAN DISK H シリーズの画面で見るマニュアルを参照いただき、一括登録ファイルを作成ください。今回は補助ツールを利用して作成した添付の「sample_特定個人運用.CSV」を利用します。
それぞれのファイルは以下のリンク先よりダウンロードください。
テンプレート
http://www.iodata.jp/solutions/whitepaper/mynumber_landiskh_sample.csv
サンプル
http://www.iodata.jp/solutions/whitepaper/mynumber_landiskh_template.csv

手順 6－2：使用量制限の有効化

個人別のバックアップフォルダーで使用量制限を行うため、使用量制限の有効化を行います。

> ⚠ 使用量制限を含む一括登録を行う場合、使用量制限が有効でないとエラーになります。

［サービス］→［一覧]をクリックください。

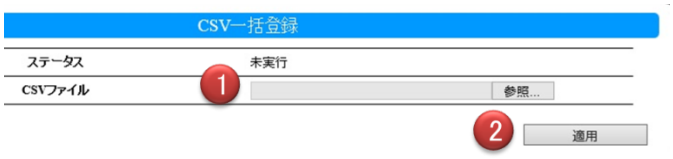
① [使用量制限]を[有効]にする。

② ［適用］をクリックする

手順 6－3：一括登録をする

作成した「sample_特定個人運用.CSV」を利用して一括登録を行います。

［サービス］→［一覧]をクリックください。



① ［参照]をクリックし、対象のCSV ファイルを選ぶ

② ［適用］をクリックする

手順 7：クローン機能の設定

手順 7－1：クローンパッケージを追加する

バックアップでクローン機能を利用するため、まずクローン機能のパッケージ追加を行います。

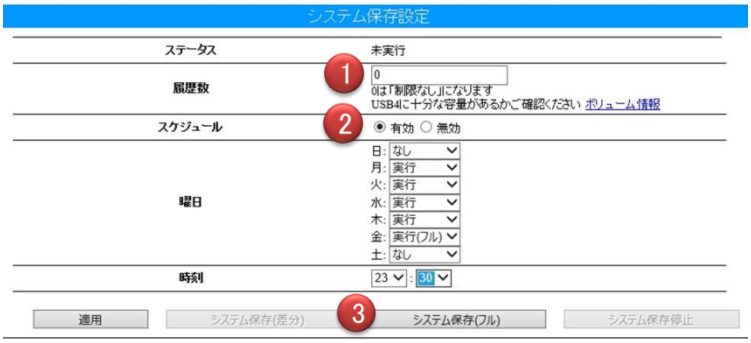
パッケージ追加は ［システム］→［パッケージ追加］→［追加］でマスター、スレーブそれぞれにパッケージを追加下さい。

① ［クローン］を選択

② ［追加］をクリックする

手順 7－２：クローン機能を設定する

［データ保守］→［クローン機能］→［システム保存設定]をクリックください。



① ［履歴数］を設定する。
② ［スケジュール］を［有効]にする。
③ ［システム保存（フル）］をクリックする

⚠ 設定後、すぐにバックアップを開始しない場合は、[適用]をクリックしてください。
⚠ 上記例は、フルバックアップを休日前の金曜日に行い、履歴差分バックアップを平日に実施しています。バックアップ可能な時刻とバックアップ容量により、組合せてご利用ください。
⚠ クローン機能を利用した場合、バックアップ先の外付 USB ハードディスクの共有フォルダーは、管理者のみアクセスできるように設定変更されます。
⚠ 復元方法についてはパッケージ取扱説明書「クローン」をご参照ください。
http://www.iodata.jp/lib/manual/pdf2/hdlh-clone-manual.pdf

今回はクローン機能を利用してバックアップを行いましたが、他のバックアップ機能（履歴差分バックアップ、レプリケーション等）を利用した場合、バックアップ先も個別にアクセス権限の設定をしてください。

以上で、導入準備・設定は完了です。

2.5 参考データ

参考１：アクセス制御

今回細かいアクセス制御を実施しましたが、それぞれの立場により共有フォルダーの見え方がどうなったかについて確認いたしました。

1. 隠し共有の確認

隠し共有設定とした「個人情報」共有フォルダーは表示されていません。

2. 特定個人情報取扱担当者（管理部 加藤部長）のケース

設定したアクセス権通り、「管理部」共有フォルダーおよび「個人情報」共有フォルダーへアクセスができました。

隠し共有設定した共有フォルダーは、「¥¥LAN DISK 名」で検索してもエクスプローラに表示されません。「¥¥LAN DISK 名¥ 共有フォルダー名」で検索すると表示されます。

今回の例では「¥¥s2fs-master¥個人情報」となります。

3. **一般社員（営業部 宇佐美さん）のケース**

「管理部」共有フォルダーおよび「個人情報」共有フォルダーへアクセスはできませんでした。
これは宇佐美さんが該当共有フォルダーにアクセス権を持たないためです。
アクセスを行おうとすると、アクセスが拒否され、アクセス権入力を求められます。

参考２：アクセスログについて

実際に保存されたアクセスログは以下のとおりです。

アクセスログ

« 前へ 1 2 3 4 次へ »

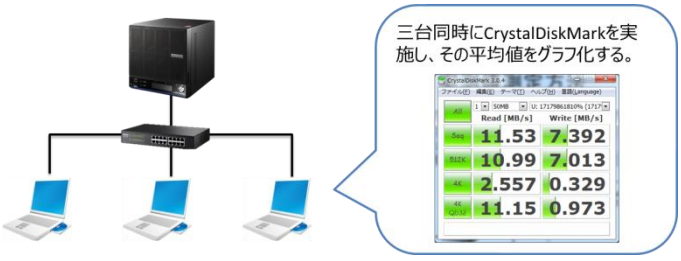
日時	ログ
2015/05/27 14:31:20	kato(192.168.52.57): open(ok): 個人情報 個人情報
2015/05/27 14:31:20	kato(192.168.52.57): close(ok): 個人情報 個人情報
2015/05/27 14:31:20	kato(192.168.52.57): open(ok): 個人情報 個人情報
2015/05/27 14:31:20	kato(192.168.52.57): open(ok): 個人情報 新しいテキスト ドキュメント.txt
2015/05/27 14:31:09	kato(192.168.52.57): close(ok): 個人情報 個人情報
2015/05/27 14:31:09	kato(192.168.52.57): open(ok): 個人情報 個人情報
2015/05/27 14:31:09	kato(192.168.52.57): close(ok): 個人情報 個人情報
2015/05/27 14:31:09	kato(192.168.52.57): open(ok): 個人情報 個人情報
2015/05/27 14:31:09	kato(192.168.52.57): open(ok): 個人情報 個人情報
2015/05/27 14:31:09	kato(192.168.52.57): connect(ok): 個人情報 個人情報
2015/05/27 14:31:08	kato(192.168.52.57): disconnect(ok): 飯田 飯田
2015/05/27 14:31:08	kato(192.168.52.57): disconnect(ok): 青山 青山

参考３：各モードの速度比較

TMNAS のリアルタイム検索、暗号化ボリュームをそれぞれ有効にした場合のクライアント３台同時接続の実測値を以下に示します。

■ 評価環境

異なる LAN DISK H の設定条件で３台のクライアントから同時にベンチマークソフト（CrystalDiskMark 3.0.4 x64）を使用して計測。



■ 測定環境

利用 HUB：ETG-ESH08NA（Gigabit 対応 8 ポート電源内蔵ハブ）

PC　【Lenovo ThinkPad E440】 OS：Windows 8.1 (64bit)
CPU：Core™ i3 4000M 2.40GHz メモリー：4.00GB

■実測値

図１．1000MB のシーケンシャルライト 5 回計測平均にて計測

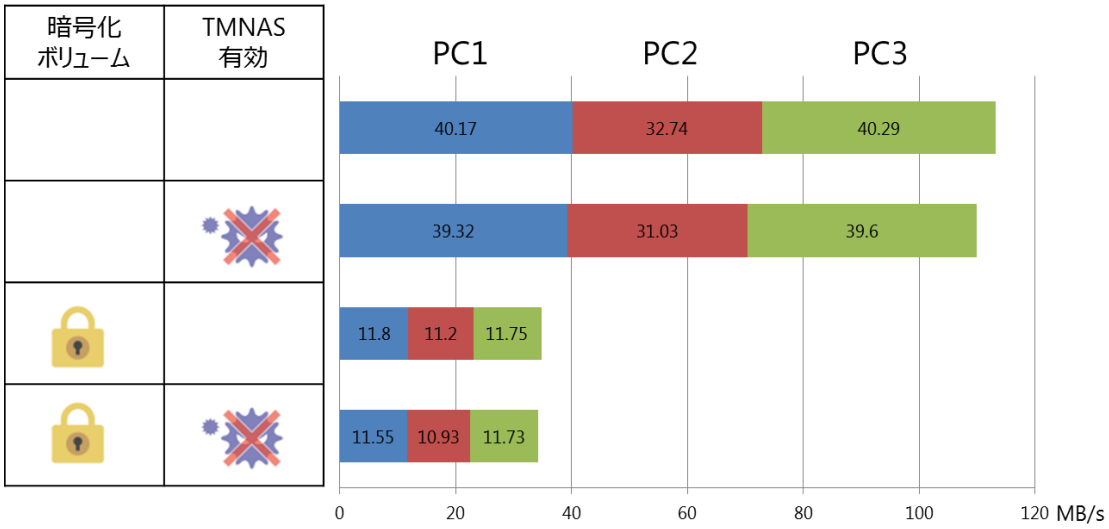
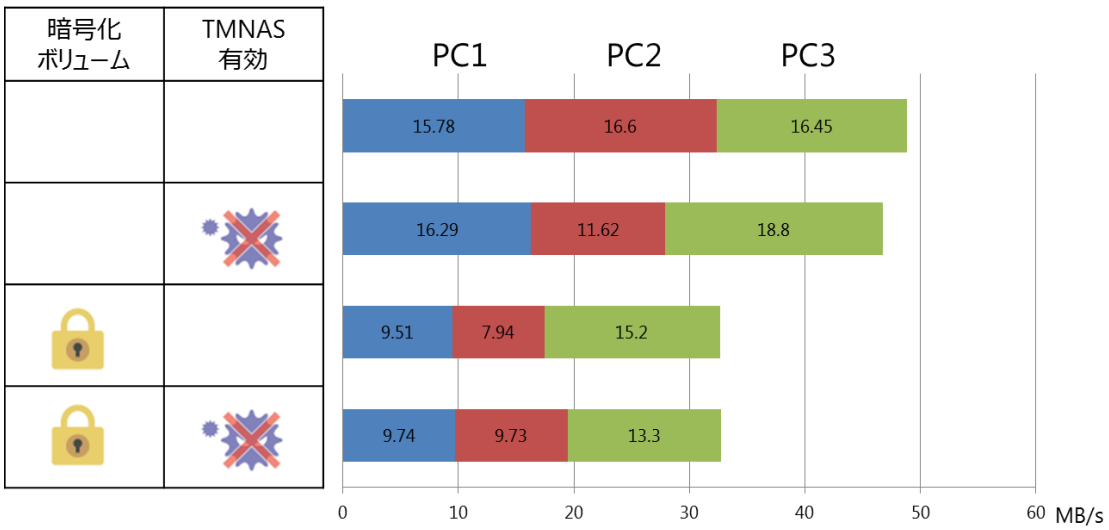


図２．1000MB の 512KB 単位のランダムアクセス ライト 5 回計測平均にて計測



LAN DISK H は複数台同時接続環境で、シーケンシャルおよびラインダムアクセスともに十分なパフォーマンスを保っていることがわかります。また、標準フォーマット（拡張ボリューム）および暗号化フォーマットの状態でも TMNAS を有効にした場合に目立った速度低下が起きていないことがわかります。
通常の運用であれば図２.のランダムアクセスの状態が通常の運用に近いため、実環境で十分なパフォーマンスを保ったままご利用いただけることがわかります。

3. 最後に

LAN DISK H は、標準設定でもご利用いただけますが、装置に装備されている各種機能をご活用いただくことで、セキュリティを高めた運用が可能になります。しかしながら、企業のセキュリティは単一機器の機能だけで保てるものではありません。組織としてセキュリティを保ち続けるには、運用ポリシーを策定し、社員ひとりひとりの意識の向上が必要となります。

今後、「個人情報保護法」や「不正競争防止法」等の改正が検討されています。マイナンバー制度の取り組みは始まりであり、企業のセキュリティの取り組みに「ゴール」はありません。今回のマイナンバー導入の取り組みを契機として、まずは現状の把握を行い、自社のセキュリティポリシーを策定の上、運用されることをお勧めいたします。

本ホワイトペーパーが、お客様のセキュリティ確保の一端になれば幸いです。