

# セキュリティ運用を軽快に実現する MistyGuardソリューション

青木 隆之\*  
(Takayuki Aoki)  
田名網 淳夫\*  
(Atsuo Tanaami)  
羽山 哲雄\*\*  
(Tetsuo Hayama)

## MistyGuard Solution: Information Security Software Easy to Use

### 要 旨

個人情報保護法施行以降、2005年にはP2P（Peer to Peer：不特定多数の個人間でやり取りするインターネットの利用形態）ファイル交換ソフトウェア経由で企業の機密情報が流出する事故が多発して社会問題となったこともあり、ほとんどの企業は何らかの情報セキュリティ対策を導入していると言われている。情報セキュリティツールの利用・運用においては利用者及び管理者に負担をかけないことが求められている。

このような背景から三菱電機インフォメーションシステムズ（株）（MDIS）はトータルな情報セキュリティ“MistyGuard<sup>(注1)</sup>”ソリューションに対して、組織及び個人としての更なる使い易さ向上を目指し、以下に示すようなバージョンアップを実施した。

#### （1）ファイル暗号化ソフト CRYPTOFILE<sup>(注1)</sup> PLUS

これまでは導入時のセキュリティ設定を変更する場合はインストールし直す必要があったが、更新プログラム（アップデート）を実行するだけでセキュリティ設定を変更できるようにした。

#### （2）PC ログオンソフト MISTYLOGON<sup>(注1)</sup> Lite

これまでは管理用サーバの導入が必須であったが、管理

サーバがなくても導入可能とした。さらに、指紋照合装置付USB（Universal Serial Bus）フラッシュメモリを使用し、メモリへのアクセスを指紋照合で制御することによって、記録されたデータの安全な持ち運びを可能とした。

（3）企業機密情報管理 DROSY<sup>(注2)</sup> Enterprise Edition 独自管理していたユーザ情報をActive Directory<sup>(注3)</sup>で一元管理できるようにした。また、ファイルサーバ内のファイルも自動で暗号化することができるようにした。

企業において情報セキュリティ管理は事業上必須になっており、情報セキュリティ運用は継続性と実効性が重要である。MDISは、今後も更に使い易く、運用し易い情報セキュリティ製品の提供に向け機能強化を継続していく所存である。

（注1）MistyGuard、CRYPTOFILE、MISTYLOGON、MELSAFETYは、三菱電機（株）の登録商標である。

（注2）DROSYは、三菱電機インフォメーションシステムズ（株）の登録商標である。

（注3）Active Directoryは、米国Microsoft Corporationの米国及びその他の国における登録商標である。



### MistyGuardソリューションの全体概要

オフィスに入室してパソコンにログオンしてから退出するまでと、退出後の情報セキュリティを確保する。

\* 三菱電機インフォメーションシステムズ（株） \*\* 三菱電機（株）

## 1. まえがき

個人情報保護法施行によって企業は自らが保有する個人情報に対する管理責任を重く受け止め、個人情報を保護する自衛策を導入している。2005年にはP2Pファイル交換ソフトウェア経由で企業の機密情報が流出するという企業の事業継続性を脅かすほどの事故が多発して社会問題となったこともあり、ほとんどの企業は何らかの情報セキュリティ対策を導入していると言われている。

これまで情報セキュリティは特別に機密性の高い情報に対してだけ必要なものとされてきたが、技術の進展と社会環境の変化によって企業では当たり前に必要なものとして位置づけられ始めている。

このような背景において、MDISでは情報セキュリティツールだけでなく、組織・個人としての使いやすさを目指したMistyGuardソリューションを提供している。

本稿では、“軽快な運用（利用）”を実現するMistyGuardソリューションについて述べる。

## 2. 企業の情報セキュリティ対策の課題

### 2.1 情報セキュリティ対策（漏えい防止）

それぞれの企業が実施している情報セキュリティ対策の内容はさまざまであるが、ほとんどの企業はまずパソコンのハードディスクやファイルを暗号化する対策を実施した。これは出張などで持ち出したパソコンやUSBメモリなどの媒体が盗難や紛失にあっても中の情報が漏えいしないための対策である。また、実際に事故が発生した場合を想定し、データアクセスなどの操作を履歴として残すツールや、パソコンからデータの書き出しを禁止するツールを導入した企業も少なくない。

### 2.2 情報セキュリティ対策（IT統制）

個人情報保護法施行後に発生した漏えい事故はファイル交換ソフトウェアを経由してパソコン内の情報が漏洩するというものが目立って報道された。技術的にはファイル交換ソフトウェアを媒介してパソコンがウィルスに感染したことが原因となり、情報セキュリティ対策として、ハードディスクを暗号化するツールを入れるだけではこのような事故は防げないことが明白となった。

これらの事故は企業の事業継続性を脅かすものとして受け止められ、それぞれの企業において情報セキュリティ対策は“情報システム”としての対策にとどまらず、企業としての統制の一部（IT統制）として取り組まれている。

<ファイル交換ソフトウェア事故の対策例>

- ① パソコンの業務用途外使用禁止  
利用禁止ソフトウェアの指定  
Windows<sup>(注3)</sup>アップデートの義務化（脆弱性抑制）

ウィルスチェックパターンアップデートの義務化（脆弱性抑制）

パソコン/媒体の持ち出し許可制度への移行

## 2.3 情報セキュリティ運用の課題

情報セキュリティ対策は実際の運用においては無理や無駄が含まれていることも多く、業務効率よりも“安全”を優先させた結果、業務上支障が生じかねない例もある。

例えば、利用者はパソコンの起動・終了時にいつもデータの暗号化処理で10分間待たされたり、パソコンのログオン時に手帳を見ながら覚えられないほど長いパスワードを入力したりしている。

また、情報セキュリティ事故発生時のリスクは利用者側にも責任分担が大きくなっている。例えば、利用者がUSBメモリでデータを社外に持ち出す場合、利用者は情報漏えいに関わる宣誓書（覚書）にサインをし、適正な管理手続き（例えば上長承認）を経ることになるが、利用者が安心してデータを持ち出すためには情報セキュリティツールによる十分な保護が必要である。一方、管理者側のコントロールも容易ではない。手続きを用意し、規制を強化してもすべての利用者にルールを守らせることは困難である。利用者の情報セキュリティ対策に対する継続的な啓蒙も重要なことであるが、目の前の情報セキュリティリスクを回避するためには情報セキュリティツールが必要となる。

結果的に、安全・安心のために情報セキュリティツールの導入は欠かせないが、その情報セキュリティツールは利用者及び管理者が運用しやすいものでなければならない。

## 3. 軽快に使えるMistyGuardソリューション

前章に述べた課題を解決するため、MistyGuardソリューションでは、情報セキュリティ対策をよりわかりやすく簡単にし、利用者の負担を軽減させる情報セキュリティソリューションを提供している。例えば、パソコン上のセキュリティ設定を更新することができたり、指紋照合装置付USBフラッシュメモリを活用することで、USBメモリ上のデータとパソコン本体の両方のセキュリティ管理等の容易化を実現している。

### 3.1 セキュリティ設定を自動更新できる暗号化ソフトウェア<CRYPTOFILE PLUS>

CRYPTOFILE PLUSは、情報セキュリティ対策の基本とされているパソコンのデータを暗号化するソフトウェアでMistyGuardソリューションの核をなす製品である。パソコンの起動及び終了時にハードディスクを丸ごと暗号化及び復号する他製品と異なり、ハードディスクへの書き込み及び読み出し時に逐次処理するCRYPTOFILE

PLUS はユーザをパソコンの起動及び終了時に 10 分も待たせることはない。さらに、リムーバブルディスクへの書き出しを禁止したり、ファイル操作の履歴を記録したりすることもできる。

CRYPTOFILE PLUS を導入した後に、暗号化やリムーバブルディスクアクセスに関するセキュリティ設定(ポリシー)を変更する場合、前バージョンまでは CRYPTOFILE PLUS の再インストール及び既に暗号化済みのファイルを復号が必要だったが、今回、ポリシー更新ファイルを作成してサーバから配布するだけで、各パソコン上のセキュリティ設定を自動更新できるようにした。ポリシー更新ファイルは改ざん防止のために CRYPTOFILE PLUS の導入時に生成されたポリシーグループ鍵で暗号化されており、ユーザによるセキュリティ設定の改変を防止している。

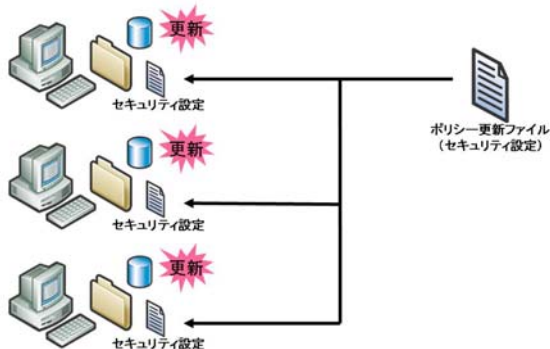


図 1 . CRYPTOFILE PLUS のポリシー更新

### 3.2 指紋照合装置付 USB フラッシュメモリでデータとパソコンを守る PC ログオンセキュリティ < MISTYLOGON Lite >

PC ログオンセキュリティ MISTYLOGON のこれまでのバージョンでは、管理用サーバを必要としていたため、簡単に導入したいお客様のニーズには応えられなかった。



図 2 . MISTYLOGON Lite の指紋照合画面

MISTYLOGON Lite では管理サーバを使用せずに、指紋照合装置付 USB フラッシュメモリでパソコンへログオ

ンすることができるよう、管理機能をパソコン内に実装している。あらかじめログオン情報 (ID・パスワード) と指紋データを関連付けることで、ID・パスワードを入力することなく、指紋照合することでパソコンに自動ログオンできるようにした。これによってユーザは覚えきれないほど長いパスワードを、手帳を見ながら間違わないように慎重に入力するようなことは必要なくなる。また、指紋データは 2 指登録できるため、指先のコンディションによる照合エラーに対応することを可能とした。

また、定期的にログオンパスワードを変更する必要がある場合は、指紋照合によって管理者ツールを実行し、関連付けたログオン情報を更新することで対応できる。

MISTYLOGON Lite の指紋照合装置付 USB フラッシュメモリは、データを安全に持ち出すための媒体としても活用することができる。指紋照合でログインすることで USB フラッシュメモリへのデータアクセス (書き込み、読み出し) が可能となるため、安全なデータの持ち運びも実現することができる。

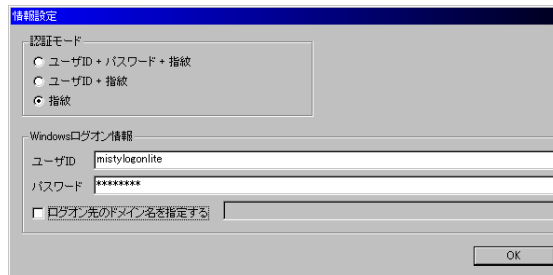


図 3 . MISTYLOGON Lite のログオン情報連携

また、ログオン履歴をログに記録し、ログを収集するオプション製品 (MISSIONLOG) と組み合わせると他の MistyGuard ソリューションと統合化されたログを参照することもできる。

MITYLOGON には指紋照合装置付 USB フラッシュメモリ以外にも IC カード (接触型・非接触型) や指紋照合装置でログオンする製品もラインアップしている。

### 3.3 企業機密情報管理 < DROSY Enterprise Edition >

企業内の機密情報を安全に共有するためのソリューションとして DROSY Enterprise Edition を提供しており、DROSY 機能で暗号化された機密文書に対して利用ユーザと操作を制限 (利用権保護) することができる。利用権保護された文書は常に暗号化された状態にあるため、万が一ファイル交換ソフトウェアなどの不正使用によって外部に流出しても機密を保持することができる。

これまでのバージョンでは導入及び運用に当たって大きく 2 つの課題があった。一つ目の課題は文書の利用権保護方法についてであり、これまでではひとつひとつの文書を

指定して DROSY 機能で利用権保護していたために手間がかかっていた。これに対し今回のバージョンでは、DROSY サーバ上の利用権保護用フォルダを使用して、そのフォルダに保存された文書を自動的に利用権保護することができる（フォルダ自動保護機能）。これによって文書を利用権保護する手間を大幅に削減することができた。この利用権保護用フォルダはサブフォルダにも対応しており、そのまま共有フォルダとしても使用できる。

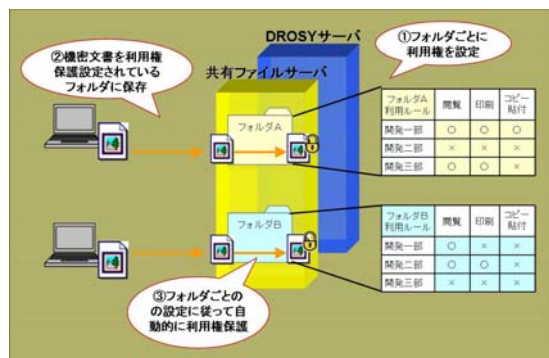


図4 . DROSY Enterprise Edition のサーバフォルダ監視による機密情報の自動変換

二つ目の課題はユーザ情報管理についてであり、これまでのバージョンでは DROSY 独自でユーザを管理する必要があった。これに対し今回のバージョンでは、Active Directory と連携してユーザ情報を一元管理することができる “Active Directory 連携アダプタ” を開発した。これによって Windows のログオンユーザ = DROSY の利用ユーザとして管理でき、ユーザ認証も統合化されるため、管理者はユーザ管理の負担を軽減できる。さらに、Active Directory のユーザグループもそのまま取込むことができるだけでなく、ユーザグループに “組織階層” を表す追加情報を定義することで階層化（最大 10 階層）された組織として取込む機能を実現している。

#### 4 . MistyGuard ソリューションの事例

本論文で紹介した 3 つの製品を含め、MistyGuard ソリューションの事例を述べる。

MISTYLOGON Lite の指紋照合装置付き USB フラッシュメモリでパソコンにログオンすることで、自動的に CRYPTOFILE PLUS、DROSY、Active Directory にもログオンしている事例を図 5 に示す。この事例ではすべてのユーザ管理を Active Directory で一元管理しており、共有ファイルサーバはドメインユーザ管理によってアクセス制御され、一部のファイルは DROSY によって利用権保護されている（フォルダ自動保護機能は未使用）。

（注 3）Windows は、米国 Microsoft Corporation の米国及びその他の国における登録商標である。

（注 4）MetaFrame は、Citrix Systems, Inc の商標である。

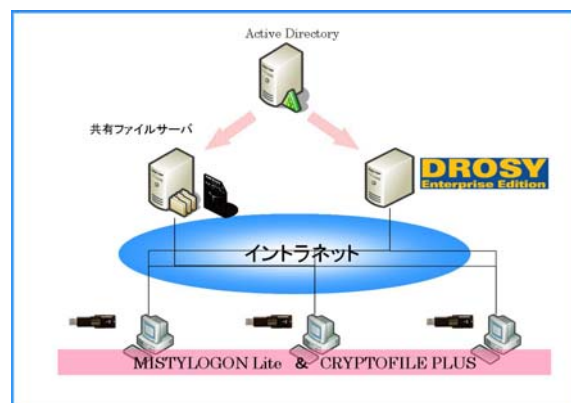


図 5 . MistyGuard ソリューションの利用事例

その他、パソコンのログオン・ログオフ、ファイル操作履歴及び入退室管理装置（三菱総合ビルセキュリティシステム MELSAFETY）からの入退室履歴を収集するログ管理システムを導入している事例や、シンクライアントを使用した MetaFrame<sup>(注4)</sup> 環境において CRYPTOFILE 及び DROSY を利用してファイル暗号化と機密情報共有をしている事例などがあり、いずれの事例も既存システムと MistyGuard ソリューションが連携してより使い易く運用し易いシステムを提供している。

#### 5 . む す び

情報セキュリティは企業にとって事業継続上、欠かせないものであり、情報セキュリティツールの使い易さ及び運用し易さが重要になっている。MistyGuard ソリューションは 2 章 3 項のような課題を解決し、セキュリティ運用を軽快にすることができる。

さらに今後は情報セキュリティ対策の継続性と実効性が重要になってくると考えており、MDIS では MistyGuard ソリューションをより一層使いやすく、運用しやすいものにするとともに、情報セキュリティによる IT 統制機能の強化を図って行く所存である。

#### 参考文献

- (1) 経済産業省：“企業における情報セキュリティガバナンスのあり方に関する研究会報告書”（2005）
- (2) 青木隆之、他：個人情報保護法、e 文書法にも対応可能なトータルセキュリティソリューション、三菱電機技報、79、No. 4、279～284（2005）
- (3) 森口修、他：機密文書の安全な公開を実現する電子文書ライフサイクルマネジメントソリューション、三菱電機技報、80、No. 4、285～288（2006）