信頼性の高い情報セキュリティ環境を構築する MistyGuard〈CRYPTOシリーズ，Missionシリーズ〉

Mitsubishi MistyGuard〈CRYPTO Series and Mission Series〉: Software for Establishing a Highly Reliable Information Security Environment

昨今，ITインフラの普及により，様々な情報漏洩(ろうえい)事件・事故が起きており，“個人情報保護法の全面施行”“プライバシー保護意識の高まり”から，情報漏洩のリスクは，事業存続を脅かすほど重大なものとなっている。ここでは，情報の漏洩・流出防止の要(かなめ)となるファイルの暗号化，持ち出し制御，アクセス履歴管理機能などを実現し，三菱電機グループほか多数の納入実績を持つMistyGuard(注)＜CRYPTOシリーズ，Missionシリーズ＞を中心に情報漏洩防止製品について述べる。

1．MistyGuard＜CRYPTOシリーズ＞

(1) MistyGuard＜CRYPTOFILE(注)PLUS＞は，世界最高水準の暗号技術MISTY(注)を用いた暗号化機能により，パソコン内のファイルを暗号化保存し，不正アクセス時の情報漏洩を防止するソフトウェアである。リムーバブルディスクへのファイルの書き出し管理，社内・組織内機密情報の安全保管，ノートパソコンの置き忘れ・盗難など，情報の漏洩・流出対策が必要な様々な場面に対応できる豊富な機能を提供する。

(2) MistyGuard＜CRYPTOFILE LOCK＞は，専用のUSBキーをパソコンに装着時だけ，リムーバブルディスクへの書き出しを可能にし，専用USBキーを管理することで，社員のリムーバブルディスクによるファイル持ち出しを制限できる。

(3) MistyGuard＜CRYPTOFILE PLUS Server eXtension＞は，ファイル共有サーバにインストールすることで，ファイル共有サーバを簡単に暗号化サーバに移行できる。クライアントパソコン上のCRYPTOFILE PLUSと連携することで，サーバ上の共有ファイルが，暗号化を意識せずに利用できる。

2．MistyGuard＜Missionシリーズ＞

Missionシリーズは，ログ管理・ファイルアクセス制御・端末ユーザー認証・ディレクトリ情報管理などを統合運用管理するサーバソフトウェア製品群である。

(1) MistyGuard＜MissionLOG(注)＞は，情報漏洩発生時の原因分析に必要なログを収集・管理するサーバソフトウェアで，CRYPTOFILE PLUS／LOCKが導入されたパソコンのログオン／オフ・ファイルアクセス・印刷・ライティングソフトウェア起動，入退室記録などの各種ログを統合管理する。

(2) MistyGuard＜MissionCRYPTO(注)＞は，サーバ上の暗号化された共有ファイルに対するアクセス制御を行う。

(3) MistyGuard＜MissionCORE(注)＞は，ユーザー情報・組織情報・アクセス権などのディレクトリ情報を管理する。

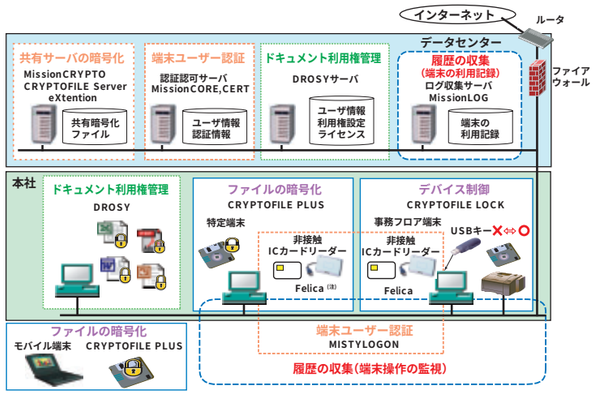
(4) MistyGuard＜MissionCERT(注)＞は，ディレクトリ情報を基にログイン時のユーザー認証とアクセス権の配布などを行う。上記(2)と(3)を組み合わせて，人事情報に連動した役割による共有フォルダへのアクセス制御を実現でき，人事異動時のアクセス権限変更も自動的に行われる。

3．その他の特長的な情報漏洩防止製品

(1) MistyGuard＜DROSY(注)＞は，電子ドキュメントを利用させたい人だけに，許可された機能範囲内で，安全に共有・公開するソフトウェアで，ドキュメントの暗号化及び利用タイミングごとにサーバ側で利用者の権限(閲覧・編集・印刷等)を確認・制御する。

(2) MistyGuard＜MISTYLOGON(注)＞は，ICカードと暗証番号及び指紋認証などを組み合わせて，確実な本人認証を実現するソフトウェアである。

以上のような多彩な製品群を組み合わせることで，信頼性の高い情報セキュリティ環境を構築することができる。



情報漏洩対策のシステム構成例

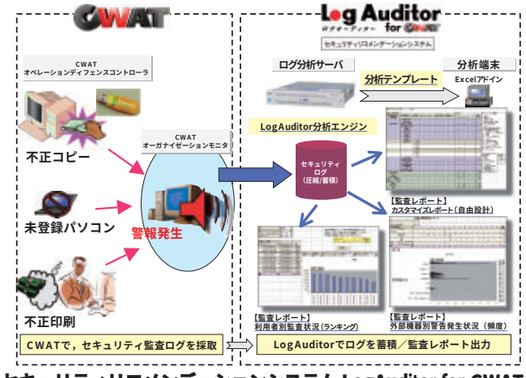
〈取り扱い：三菱電機インフォメーションシステムズ㈱ TEL：03−5445−7733〉

セキュリティリコメンデーションシステム“LogAuditor for CWAT”

LogAuditor for CWAT：Security Recommendation System

最近の情報漏洩(ろうえい)犯罪は，外部からの不法侵入から，内部の意図的な漏洩へと変化している。これに対応するには，コピー禁止などの機能を強化するだけでなく，内部の情報の取扱いに関するルール(ポリシー)の不断の改善が必要になる。

情報漏洩対策システムCWAT(注)は，パソコンの動作を監視し，不正なコピーや印刷を無効にするとともに，操作ログを採取することで，内部からの意図的な漏洩を抑止・防止する。セキュリティリコメンデーションシステムLogAuditor(注)for CWATは，CWATが採取するセキュリティログから内部情報を取り扱う利用者の動向を把握し，情報システムの運用状況を監査するレポートを出力する。日々大量に発生するログ情報から高速かつ多次元的に分析を行うことで，情報セキュリティ管理システム(ISMS)で規定されている運用モデルのPDCA(Plan-Do-Check-Action)を強力に支援する。これにより，企業における情報セキュリティポリシーの設計・実行・監視とレビュー・改善を具現化する。監査レポートは，Excelアドインツールで作成でき，ユーザーの運用形態に合わせた編集が容易にできる。また，ログを明細レベルで蓄積しており，監査証跡として，特定ファイルへの操作履歴のトレース等の出力も可能である。



セキュリティリコメンデーションシステム LogAuditor for CWAT

〈取り扱い：三菱電機インフォメーションテクノロジー㈱ TEL：03−6414−8143〉

システム障害のビジネスへの影響を最小限にするITマネジメントシステム“MDIT²SM”

MDIT²SM：IT Management System Minimizing Business Impact of System Failure

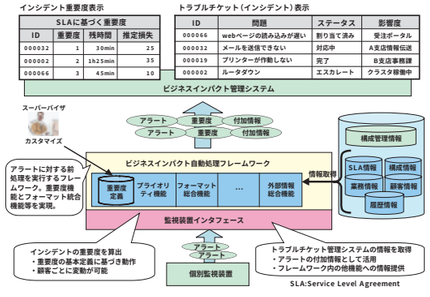
ビジネス環境のIT化が進んだ現在，ITサービスの効率化と高度化はますます重要となっている。その中で組織のITサービスプロセスの実現と運用を支援するのがITサービスマネジメント(ITSM)である。

従来のITSMではIT機器の故障に対する修理や不具合改善の効率的な処理に重点が置かれていた。しかし，ビジネス遂行の立場からは，IT機器で稼働している業務・サービスの停止がビジネスに与えるインパクトを管理する視点でのマネジメント(ビジネスインパクトマネジメント)が必要になってきている。ビジネスインパクトマネジメント機能は，ユーザー視点での運用サポートを実現し，IT機器の障害がどのような業務やサービスに影響を与えるかをリアルタイムで把握し，必要なマネジメント情報を提供する。

今回改良開発したITマネジメントシステム(MDIT²SM)は，ビジネスインパクトマネジメント機能を持つITSMを提供し，障害発生時に統合管理装置や障害監視装置が収集したインシデント(アラート)に対し，以下の一連の処理を実行可能とした。

- インシデントに対する関連情報の自動収集
- インシデントの内容判別
- インシデントに対応した処理手順の実行
- インシデントに対応した新たな処理手順の追加や変更

上記により，障害発生時に関連情報を解析／判断し，バックアップ処理／縮退処理／代替処理などを自動実行させることにより，業務への影響を最小限に抑えることができる。



障害発生時のビジネス影響分析の流れ

〈取り扱い：三菱電機インフォメーションテクノロジー㈱ TEL：03−6414−8191〉