

要旨

お客様にとって快適・安心で発展性のあるセキュリティ対策の実現を目指して、三菱電機インフォメーションシステムズ株式会社(MDIS)は、“三菱電機のトータルセキュリティ体系”<sup>(1)</sup>に基づき、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を開発した。

その主要なコンセプトは、マネジメントのPDCAサイクルと情報資産のライフサイクル全体をカバーし、物理的対策や紙への印刷権限管理などの人的対策も含め、“導入の検討から構築・運用・監査”までをトータルに提供する“ワンストップサービス”を実現することである。

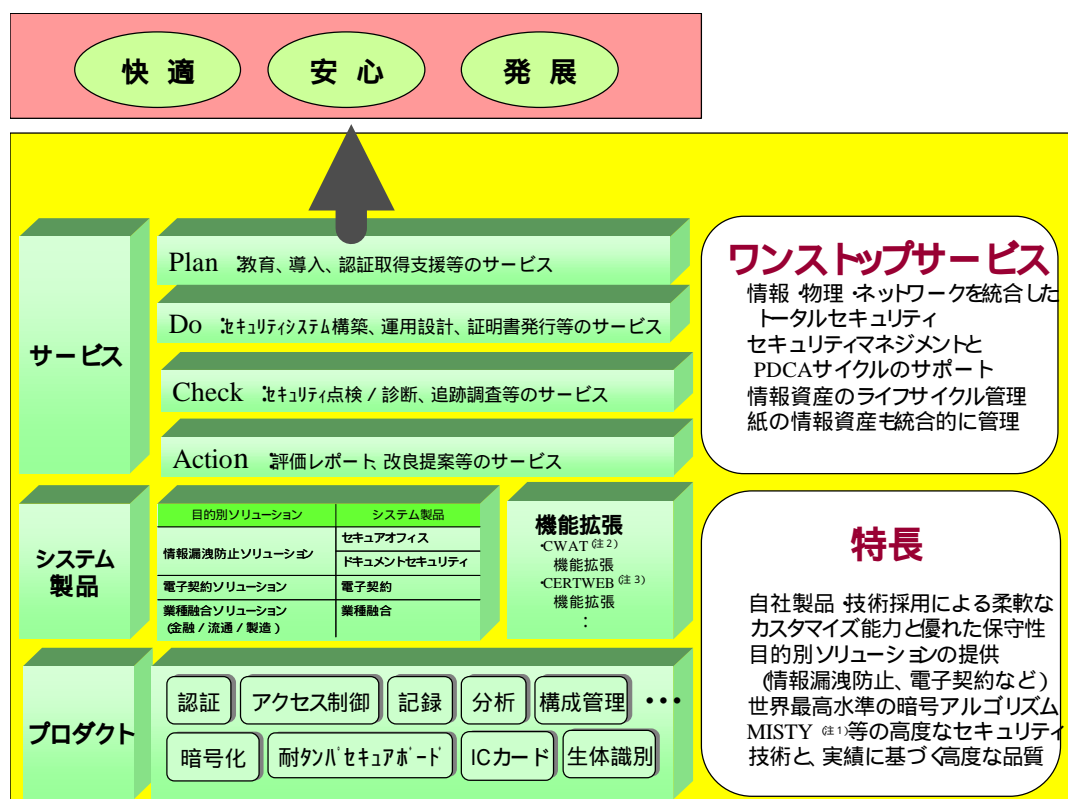
本ソリューションでは、業務要件に合わせたカスタマイズへの柔軟な対応と、官公庁を中心とした実績を活かした

高品質ソリューションを特長としているが、新たに導入や運用が容易でかつ経済的な目的別ソリューションを追加した。本稿ではその中の個人情報保護法とe文書法に対応する2つの目的別ソリューションを紹介する。

“情報漏洩防止ソリューション”は、個人情報保護法が求める安全管理措置の様々なニーズに応じた段階的な導入を可能としており、ファイルの暗号化や入退室管理などを統合したセキュアオフィスシステムと印刷制御などの機能を持つドキュメントセキュリティシステムを核に提供する。

“電子契約ソリューション”は、電子署名法とe文書法によって契約書等の電子保存が可能となったことを受け、電子文書の真正性を高める電子署名と電子署名有効性延長の機能を組み込んだ電子契約システムを核に提供する。

(注1) MISTYは、三菱電機㈱の登録商標である。  
(注2) CWATは、インテリジェントウェブ社の登録商標である。  
(注3) CERTWEBは、(株)三菱電機ビジネスシステムの登録商標である。



MDIS が提供するトータルセキュリティソリューションのイメージ

MDISが提供するトータルセキュリティソリューションは、大別してプロダクト、システム製品及びサービスから構成される。統合的対策、PDCAサイクルサポート、情報資産のライフサイクル管理、紙の情報資産の統合的管理等をワンストップでサービスし、高度なセキュリティ技術と品質、自社製品・技術採用による柔軟なカスタマイズ能力と優れた保守性等の特長を有する。

## 1. ま え が き

真にソリューションと言えるセキュリティソリューションを提供するためには、主に次のような課題がある。

- (1) 情報・物理・ネットワークを統合したトータルセキュリティを提供するワンストップサービスが必要。
- (2) マネジメント・情報システム・情報自身のライフサイクル全体をカバーするワンストップサービスが必要。
- (3) コストパフォーマンスも含め、お客様に最適なソリューションを提供するため、迅速・柔軟なカスタマイズや目的別ソリューションを提供するワンストップサービスが必要。
- (4) 電子情報だけでなく、印刷や紙の電子化・保存に係わる紙の情報資産も統合的に管理するためのドキュメントセキュリティを提供するワンストップサービスが必要。

本稿では、これらの主要課題の解決を図るトータルセキュリティソリューションについて、そのコンセプト及びフレームワークを紹介するとともに、構成要素である目的別ソリューションの中の“情報漏洩防止ソリューション”及び“電子契約ソリューション”について紹介する。

### 2. トータルセキュリティソリューション

本章では、MDIS が提供するトータルセキュリティソリューションのコンセプト及びフレームワークを紹介する。

#### 2.1 ワンストップサービスの提供

三菱電機グループでは、情報セキュリティ、物理セキュリティ、ネットワークセキュリティを統合したトータルセキュリティを提供している。情報セキュリティでは、世界最高水準の暗号アルゴリズム MISTY を開発して以来、暗号技術を中心としたセキュリティ製品を創出してきた。昨今の個人情報漏洩の社会問題化によるセキュリティ強化への要求に応えるため、長年培ってきたセキュリティに関連するノウハウを結集し、“導入検討から構築・運用・監査”までをトータルにワンストップでサービスすることも特長としている。

#### 2.2 PDCA サイクルのサポート

セキュリティは、規則の整備や情報漏洩防止製品を導入することが重要であるが、更に導入後の点検・監査により“守られている”ことを日々チェックする必要がある。そのため、P (Plan) ・D (Do) ・C (Check) ・A (Action) を定期的実施するための仕組み作りが重要である。MDIS は、情報セキュリティマネジメントシステム (ISMS) やプライバシーマークの認定取得コンサルティングで、多くの企業に対する支援を行い成果を挙げてきた。また、それらの監査時に必要となる評価報告書の作成を支援するサービスも行っており、導入及び構築だけでなく、PDCA サイクル全般に亘ったサービスとして提供している。今後は、企業にとって守るべき

情報資産全般に対し、どのような脅威が存在するか等を分析し、PDCA に沿った管理面及び技術面の総合対策も提案していく (図1)。

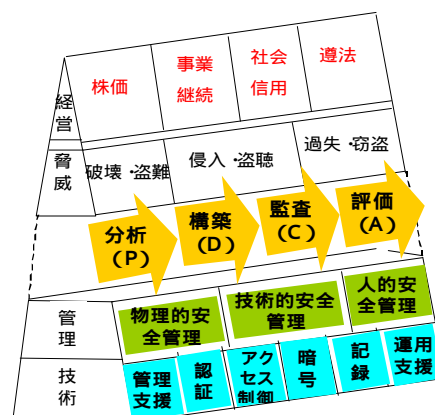


図1. PDCA サイクルの考え方

### 2.3 情報資産のライフサイクル管理

情報資産については、発生から廃棄までのライフサイクル ILM (Information Lifecycle Management) が存在する。パソコンは、ネットワーク接続されて情報の共有が行われているため、情報が廃棄されるまで漏洩の危険は内在している。そこで、情報資産の全ライフサイクルに亘り漏洩を防止するソリューションを提供することとした。このトータルセキュリティソリューションのフレームワークを表1に示す。暗号やアクセス制御を行うプロダクト、各プロダクトを融合したシステム製品及び導入から評価までのサービスにより、ハイレベルなセキュリティを提供している。

#### 2.4 ドキュメントセキュリティへの対応

情報セキュリティと言うとインターネットを中心とした電子データ (ディスク上のファイル等) に注目がいく。

ところが、実際の情報漏洩はプリントアウトされた紙も漏洩するケースが多い。また、2005年4月施行のe文書法によって、従来は紙で保存が義務付けられていた文書の電子化保存が可能となる。そのため、トータルセキュリティソリューションでは、電子文書の印刷時の制御と権限管理、保存された電子文書の改竄防止にも対応している。

#### 2.5 ソリューションの特長

##### (1) 柔軟な対応

サービスからプロダクトまで、ほとんどのコンポーネントを当社グループが開発・提供しているため、顧客の業務要件に合わせたカスタマイズに応えられる。セキュリティを強化する目的から、従来の業務諸習慣を変更すると操作が面倒等の理由から、結局、セキュリティを無視することになり易い。

MDIS では、導入の実効性を高めるため各企業の実態に合わせたソリューションを提供している。また、プロダクトは

表1. MDIS が提供するトータルセキュリティソリューションのフレームワーク

情報ライフサイクル		収集・取得	入力	保管	参照	更新	バックアップ	持ち出し	預託	配布	送付・伝送	監査	廃棄	
安全性への配慮		利用目的の明確化	秘匿レベルの設定	真正性の確保	参照者の特定印刷許可	更新者の特定	媒体保管の監視	持出者の特定	機密保持契約	誤配信防止	利用履歴の収集	定期的実施	廃棄証明取得	
脅威 存在する	破壊・盗難			サーバ盗難			媒体盗難	PC盗難	資料/媒体盗難		サイバーテロ		媒体盗難	
	侵入・盗聴		盗聴	不正アクセス	成りすまし	成りすまし				盗聴	ウイルス盗聴	成りすまし		
	過失・窃盗	窃盗	過失	窃盗	印刷持出	過失	窃盗	媒体持出		過失			窃盗	
犯罪対策	経営者	防衛・防御	入力者権限	改竄防止	アクセス権限	アクセス権限	保管場所	許可制	契約	社外配信規定	ネットワークガード	監査	証明書	
	従業員	検知・捜査	5W1Hログ	監視	5W1Hログ	5W1Hログ	監視	5W1Hログ	定期監査	5W1Hログ	ネットワークガード	監査	証明書	
	従業員	抑止・防犯	検認	秘の 設定	権利認証	権利認証	定期保存	暗号	提供媒体管理	暗号			定期巡回	
サービス	Plan	セキュリティ教育	コンサルティング/テンプレート/実践塾 / e-Learning/ プライバシーマーク取得塾											
		ISM取得												
	Do	セキュリティ導入	セキュリティ・エキスパート(e-Consulting)/セキュリティまんが読本											
		認証書発行	プライベートCA/RA運用 (ICカード, eTRON <sup>(注4)</sup> )											
		不正アクセス監視	ポリシー違反監視											
		セキュリティシステム構築	セキュリティシステム構築サービス											
		運用設計サービス	運用設計サービス											
		通信インフラ構築 (WLAN, VPN, FW, IDS, IDP)	サーバ/ネットワーク/インフラ構築運用支援サービス											
	Check	機密ファイル保管	機密ファイル管理/長期保存											
		セキュリティ点検/診断	情報追跡サービス(ドキュメント・トラッキング)											
Action	追跡調査													
	評価レポート	評価レポート												
システム製品	目的別ソリューション	情報漏洩防止ソリューション	セキュアオフィス										セキュアオフィス	
		電子契約ソリューション	ドキュメントセキュリティ											
	機能拡張	業種融合ソリューション (金融/流通/製造業)	電子契約										業種融合	
		CWAT機能拡張	業種融合										業種融合	
機能拡張	CERTWEB機能拡張	CWAT機能拡張 (ログ機能/暗号機能)										CWAT		
トータルセキュリティソリューション	認証	認証書発行												
		eX書法対応												
		ICカード/指紋LOGON												
		入退室管理												
		ディレクトリ連携												
		モバイル管理												
		SBC												
		FW												
		ウイルスバスター												
		サーバ機密情報格納												
	プロダクト	暗号	利用権管理											
			印刷制御											
			Web画面制御											
			メール管理											
			逐次暗号											
		記録	操作ログ											
			DS											
			DP/MSIESER <sup>(注5)</sup>											
			監視カメラ											
			バージョン確認											
構成管理	構成管理													
	自動配布ツール													
	ポリシー自動作成													
	ログ分析													
	ポリシー強化													

<備考> 情報ライフサイクル管理 (ILM) に基づいてサービス及び製品の提供範囲を示す。“○”、“ ” は、サービス・システム製品・プロダクトの各ソリューションが対応しているライフサイクルの範囲を示す。

- ISMS : Information Security Management System
- CA/RA : Certificate Authority/Registration Authority
- WLAN : Wireless Local Area Network
- VPN : Virtual Private Network
- FW : Fire Wall
- IDS : Intrusion Detection System
- IDP : Intrusion Detection and Prevention
- SBC : Server Based Computing

(注4) TRON は、社団法人トロン協会の登録商標である。  
 (注5) MSIESER は、三菱スペース・ソフトウェア(株)の登録商標である。

単機能で製品化しており、必要な機能に絞った構築を可能としているため、無理のない導入が行える。

## (2) 高品質ソリューションの提供

当社グループは、暗号アルゴリズム MISTY を開発して以来、官公庁を中心に、暗号や認証プロダクトの提供及びセキュリティシステムの構築を数多く経験してきた。トータルセキュリティソリューションは、その実績をベースとしているため、高品質なソリューションであり、導入・運用の容易性や経済性等も考慮している。

## (3) 目的別ソリューションの創出

“セキュリティは必要だが何から手を付けたらよいかかわからない”と言うお客様のために、目的別ソリューション（システム製品）を創出して、導入から運用・監査までをスムーズに行なえるようにしている。本稿では目的別ソリューションのうち、次の2つを紹介する。

### 情報漏洩防止ソリューション

2005年4月施行の「個人情報の保護に関する法律」（個人情報保護法）に対応したソリューションであり、各府省のガイドラインに沿った段階的な導入を可能としている。

### 電子契約ソリューション

2005年4月施行の「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律及び民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（e文書法）に対応したソリューションである。なお、上記の情報漏洩防止ソリューションのシステム製品であるドキュメントセキュリティもe文書法に関連している。

## 3. 目的別ソリューション

### 3.1 情報漏洩防止ソリューション

#### 3.1.1 目的

“情報漏洩防止ソリューション”は、個人情報保護法に対応するため、情報資産のライフサイクルILM全般に亘る情報漏洩防止対策を導入から運用・監査まで容易でかつ経済的に実施できるようにすることを目的としている。このため、各府省の個人情報保護ガイドラインに沿って段階的に導入できる様に機能をコンポーネント化している。なお、不正競争防止法に対応した企業機密管理にも活用できる。

#### 3.1.2 機能と構成

情報漏洩防止ソリューションの機能構成例を図2に示す。

#### (1) 情報セキュリティコンポーネント

ファイル暗号化システム CRYPTOFILE<sup>(注6)</sup>PLUS・MissionCRYPTO<sup>(注7)</sup>：特定フォルダ等の一括暗号化・自動暗号化を可能とする。共有サーバ上で機密情報を暗号化し

て保管し、人事情報に連動した役割（ロール）によるアクセス制御も実現する。

利用権管理システム DROSY<sup>(注8)</sup>：各種文書ファイルのユーザごとの利用権管理（暗号／復号・印刷・閲覧・更新等）を可能とする。

デバイス制御ソフトウェア CRYPTOFILE LOCK：USBメモリ、DVD等のリムーバブルメディアへの書込み禁止制御を可能とする。

デスクトップセキュリティ MISTYLOGON<sup>(注6)</sup>：ICカード・指紋・パスワード・PKI認証等の多様なユーザ認証手段を提供する。

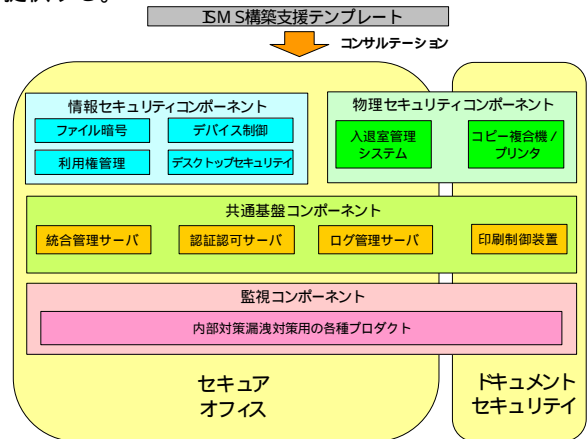


図2. 情報漏洩防止ソリューションの機能構成例

#### (2) 物理セキュリティコンポーネント

入退室管理システム MELSAFETY<sup>(注6)</sup>：IDコントローラが個人のアクセス制御情報を持ち、指紋照合等のユーザ認証手段により入退室を管理する。ユーザ情報・アクセス制御情報は、統合管理サーバで一元管理が可能である。

コピー複合機/プリンタ：ネットワークに対応し、イメージスキャンにより紙文書を電子化して保管する機能とクライアントからの印刷指示を制御する機能を提供する。利用権管理システムと組み合わせ、ICカードを用いたユーザ認証によるコピー・印刷・スキャンの制御が可能となる。

#### (3) 共通基盤コンポーネント

統合管理サーバ MissionCORE<sup>(注7)</sup>：情報セキュリティ及び物理セキュリティのユーザ情報及びアクセス権情報を一元管理し、管理者向けの統合運用管理ツールも提供する。

認証・認可サーバ MissionCERT<sup>(注7)</sup>：統合管理サーバで管理されているユーザ情報及びアクセス制御情報を基に、ファイル暗号化システムと利用権管理システム等に対してユーザ認証と認可決定を行う機能を提供する。

ログ管理サーバ MissionLOG<sup>(注7)</sup>：いつ、誰がどのように情報にアクセスしたのか、入退室したのか等を分析するためのログ情報を、収集・保管する機能を提供する。

印刷制御装置 PageACSES PRO：利用権管理システム DROSY をベースとした文書利用許可機能をコピー複合機/プリンタに組み込み、ICカードを用いてユーザ認証され

(注6) CRYPTOFILE、MISTYLOGON、MELSAFETYは、三菱電機㈱の登録商標である。

(注7) MissionCRYPTO、MissionCORE、MissionCERT、MissionLOGは、三菱電機インフォメーションシステムズ㈱が商標出願中である。4

(注8) 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。

た個人単位に、印刷・FAX・スキャン時の利用権許可設定・権限実行機能を提供する。

#### (4) 監視コンポーネント

内部情報漏洩対策システム CWAT：ネットワークと端末操作の両者を監視し、防御・集中監視制御を実現する。未登録パソコンの接続監視機能、端末に接続された外部記憶装置、印刷処理、オペレータの行動パターン認識による特異挙動などの監視機能及び集中的なイベント管理機能を提供する。

#### 3.1.3 特長

(1)種々のリスクに対して網羅的に機能を提供している点が大きな特長であり、目的や規模に応じて、大規模なイントラネットシステムから特定用途向きの小規模システムまで迅速・的確な構築が可能となる。

(2)世界最高水準の暗号アルゴリズム MISTY 等の技術を駆使して、暗号化・ユーザ認証・アクセス制御・利用権制御を実現している。

(3)1枚のICカードで、入退室やパソコンログオン等の種々のユーザ認証を統合可能とし、セキュリティと利便性の両立を実現している。

(4)ユーザ情報及びアクセス制御情報を一元管理し、人事異動・ポリシー変更等に伴う運用管理コストを抑制できる。

(5)各コンポーネントのログ情報を収集し、ISMS の認定に必要な統一形式で集中管理ができる。

#### 3.1.4 システム製品

##### (1) セキュアオフィス

図2の物理セキュリティコンポーネントの“入退室管理システム”と各種セキュリティコンポーネントを組み合わせたシステム製品が“セキュアオフィス”である。

図3に、セキュアオフィスを利用して、広域に分散した拠点における入退室管理と、パソコンのセキュリティ管理を、全社で集中管理するシステムの構築例を示す。人事異動時の変更管理や障害・災害対策も考慮した例である。

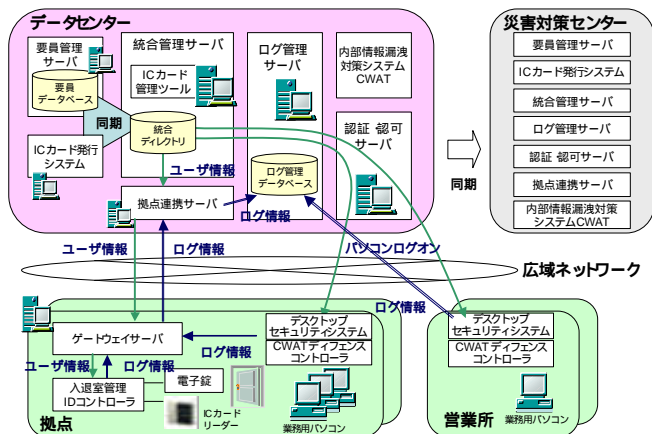


図3. 大規模なセキュアオフィスのシステム構成例

社員証ICカードによる入退室とパソコンのユーザ認証：入退室・パソコンへのログオンを統一的に実現している。

ユーザ情報・アクセス制御情報の一元管理：全従業員のユーザ管理及び入退室・パソコンログオンのアクセス制御情報を、データセンターで一元管理するため、障害や災害対策等の二重化構成時の変更管理や運用のコスト抑制、セキュリティポリシーの統一等を実現している。

一括管理された要員データベースと同期した入退室管理：人事異動等に伴う社員証ICカードの発行・失効・権限変更に関連し、各拠点入退室管理IDコントローラに自動反映する。

CWATによる端末とネットワークの監視：内部情報漏洩対策システムCWATをパソコンとネットワークに適用し、端末での持出しや印刷、登録外パソコン接続等の監視機能及び各セグメント内で行われるネットワーク入出力の監視機能を提供する。

ログ情報の一元管理：拠点に配置したゲートウェイ端末を経由して、ISMS の認定に必要な形式の入退室・パソコン操作のログ・端末監視・ネットワーク監視情報及び入退室管理装置の状態を収集し、データセンターでの集中管理を行う。

##### (2) ドキュメントセキュリティ

図2の物理セキュリティコンポーネントの“コピー複合機/プリンタ”と各種セキュリティコンポーネントを組み合わせたシステム製品が“ドキュメントセキュリティ”である。

図3に、ICカードを利用した個人認証と、紙文書から電子ファイルまでのトータルな文書利用許可管理を実現するドキュメントセキュリティのシステム構成例を示す。

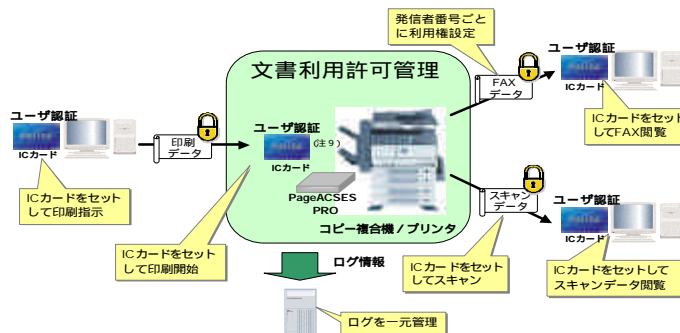


図4. ドキュメントセキュリティのシステム構成例

コピー複合機等と情報セキュリティとの連携により、次の特長を持つドキュメントセキュリティを提供している。

ICカードを用いた個人認証に基づいて、コピー複合機/プリンタの利用者を限定できる。

電子ファイルの暗号化・利用権許可設定等によって、機密文書ファイルを安全に共有できる。

印刷物の置忘れによる盗み見を防止する。出力指示時に指定したICカードに対して印刷許可を設定し、同じICカードをプリンタにセットすると印刷が開始する。

閲覧権限者設定とICカードによる個人認証によって、受信FAX文書の不正閲覧を防止できる。

スキャンしたファイルは、自動的に暗号化され利用権設定されるので、電子化リスクが低減する

(注9) Felicaは、ソニー(株)の登録商標である。

ログ情報の一元管理： ～ のコピー・印刷・スキャン・閲覧を、いつ・だれが実施したかについて一元管理できる。

### 3.2 電子契約ソリューション

#### 3.2.1 目的

契約書は押印と書面での保管が必要なことから、従来は紙の文書で交換していた。2001年施行の電子署名法により、印鑑による押印は、電子証明書による電子署名に置換でき、2005年4月施行のe文書法によって、電子署名を含めた一定の条件を満たせば、紙で保管していた文書を電子保管することも可能となった。契約書の電子化により、基幹システムとのシームレスな連携、閲覧・検索性の向上、保管費用の削減、紙の契約書による受渡し等が無くなることによるスピードアップや郵送料削減が期待できる。

#### 3.2.2 特長と構成

電子契約の流れは社内及び会社間のワークフローとして推移するが、その電子署名と保管部分に対して、ワークフローシステムと連携可能なシステムを提供する。

##### (1) 電子署名ソフトウェア SignedPDF<sup>(注10)</sup> ファミリー

電子契約で必要となる電子署名の機能をあらゆる局面で提供するソフトウェアである。具体的な特長を以下に示す。

見読性に優れたPDF(Portable Document Format)を対象としており、従来の紙による契約書のレイアウトをそのまま利用できるため、紙の契約書から電子契約への移行がスムーズに図れる。

クライアントには、PDF生成などの特別なソフトウェアは不要(但し、閲覧用ソフトウェアは必要)なので従来の電子契約システムに比べ、導入費用が1/10程度になる。

サーバ上の電子契約ワークフローへ組み込むための簡易なAPI(Application Program Interface)を提供する。

電子署名、署名検証を、高速かつ自動で処理する。

##### (2) 電子署名有効性延長サーバ EVERSIGN<sup>(注10)</sup>

電子署名に必要な電子証明書には有効期限があり、一般には1～3年間である。電子契約書の種類によっては、その有効期限を超えて長期に保存する必要があるため、EVERSIGNは電子署名の有効性を延長する機能を提供する。図5に、電子署名有効性延長の原理を示す。

電子商取引推進協議会(ETC)が2003年3月に発表した電子署名文書長期保存に関するガイドラインで推奨されている長期保存用電子署名フォーマット(RFC3126)及びタイムスタンプフォーマット(RFC3161)を採用している。公開されている業界標準仕様を採用しているため、電子署名文書を公正に長期保存することが可能となる。

予め指定された条件で、個々の電子証明書の有効期限をチェックし、自動的に再延長処理を行なう。

電子契約ワークフローや電子契約書ファイリングシステムとの連携用インタフェースを提供する。

との連携用インタフェースを提供する。

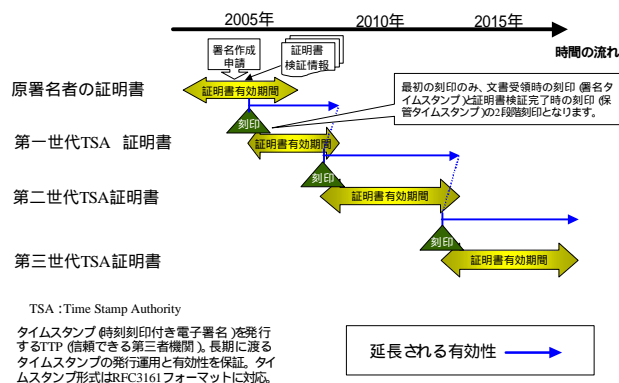


図5. 電子署名有効性延長の原理

#### 3.2.3 システム製品(電子契約システム)

電子署名と電子署名有効性延長の機能を組み込んだシステム製品が“電子契約”であり、その構成例を図6に示す。

電子契約時点で、電子署名検証で証明書を受領し、PDFで署名後、契約受付処理でタイムスタンプを自動付与する。

書面契約の場合は、契約受付時にスキャナで電子データ化後にPDF署名し、以後は上記の電子契約と同様となる。

社内稟議(ワークフロー)を経た上で、電子ファイリングに登録される。

1～3年後の署名有効期限間近になると、EVERSIGNが予め指定された条件で自動的に署名延長する(新たなタイムスタンプが付与されて有効期間が延長される)。

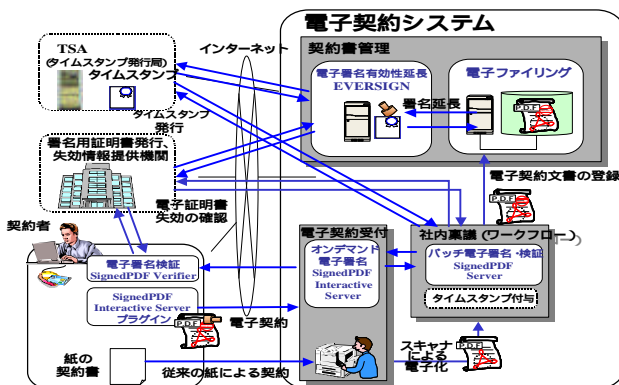


図6. 電子契約のシステム構成例

## 4. むすび

ワンストップサービスを実現するMDISのトータルセキュリティソリューションの概要を紹介した。今後は、お客様業務及び利用者の負担を極小化する“より快適なソリューション”に向けて、自動化・統合化・ユーザフレンドリーなインタフェース等に磨きをかけて行く所存である。

### 参考文献

- (1) 市毛正行, ほか: 三菱電機トータルセキュリティソリューションの推進, 三菱電機技報, 78, 8, 500~504 (2004)

(注10) SignedPDF、EVERSIGN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。