

セキュリティ技術を活用した トータル Web インテグレーションフレームワーク “セキュア Web ソリューション”

田名網淳夫* 角野 章之**
遠藤 淳* 釜坂 等***
鷲津 忍*

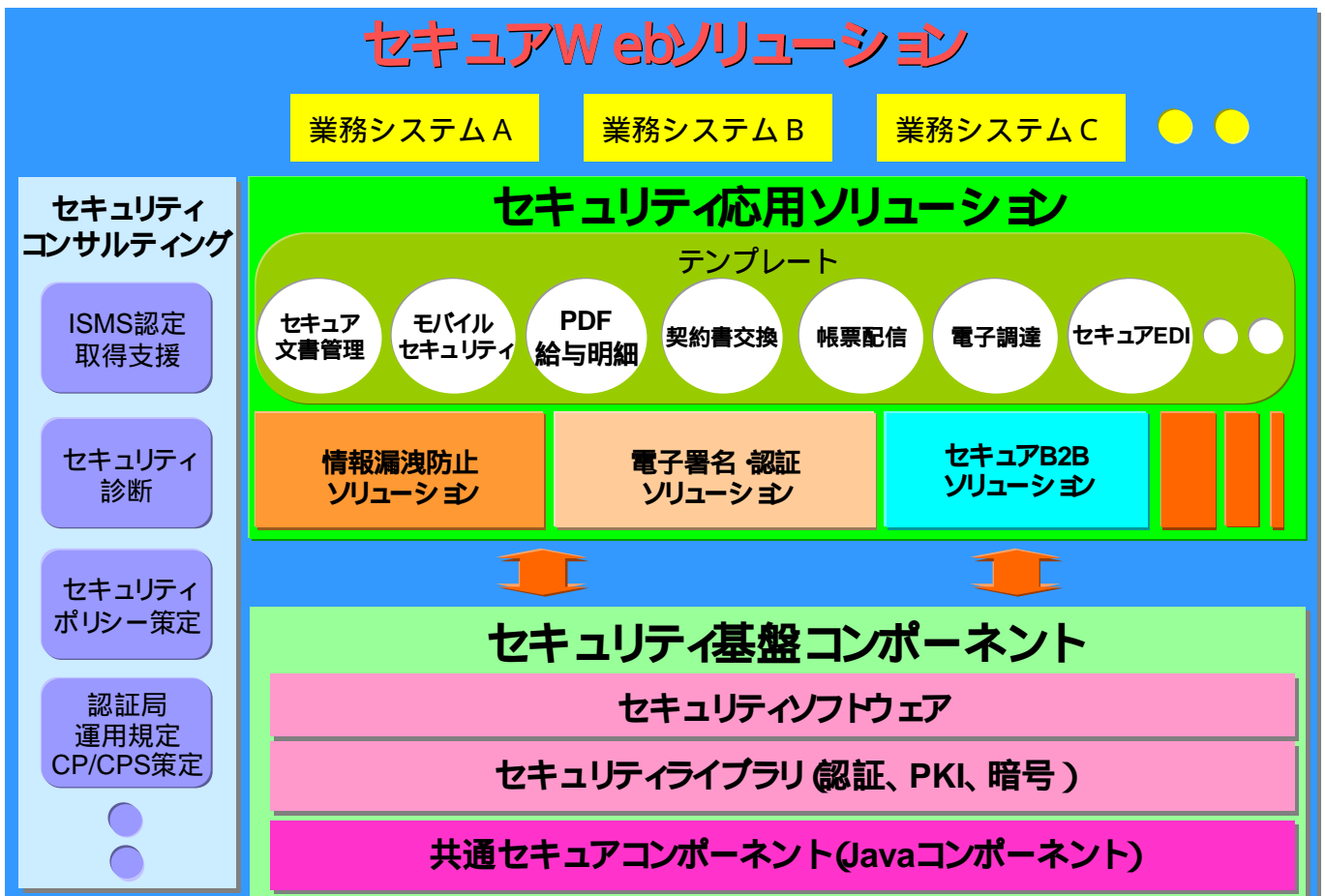
要 旨

インターネットの普及、Java 仕様の成熟化などにより、Web ベースのシステムニーズが拡大しており、これまで困難とされていた基幹系システムを Web ベースで再構築する事例も増えている。Web ベースのシステムはプラットフォーム依存度が低く、システム開発費用、運用費用を抑制できるなど多くの利点があげられる。一方で、Web は情報公開・共有技術として開発されたものであるため、サーバへの不正アクセスやデータの盗聴などセキュリティ上のリスクが多いことも事実である。また、セキュリティに対する企業の関心が高くなり、すべてのシステムにセキュリティが求められるといっても過言ではない。

三菱電機インフォメーションシステムズ(株) (MDIS) では Web ベースシステムのセキュリティ上の課題を解決したり、情報システムにセキュリティ機能を実装するためのフ

レームワークとして、“セキュア Web ソリューション”を提供している。セキュア Web ソリューションは、人的・物理的な側面も含めた情報セキュリティシステムを構築するためのセキュリティコンサルティング、PKI (Public Key Infrastructure : 公開鍵基盤) 関連ライブラリをはじめとするセキュリティ基盤コンポーネント、情報漏洩の防止やセキュアな B 2 B (Business To Business) 環境及びこれらの活用ノウハウを集積したセキュリティ応用ソリューションから構成される。

MDIS のセキュア Web ソリューションは、これまでに蓄積した Web 技術とセキュリティ技術を活用して、特にセキュリティリスクに対する企業情報システムの多様なニーズにも対応できる安全で安心な Web ベースのシステムインテグレーションサービスを提供する。



ISMS : Information Security Management System、CP : Certificate Policy、
CPS : Certification Practice Statement、PDF : Portable Document Format、PKI : Public Key Infrastructure
EDI : Electronic Data Interchange

セキュア Web ソリューションの体系図

この図は、セキュア Web ソリューションの体系を示したものである。情報セキュリティシステムの構築コンサルティングサービスと、セキュリティ基盤コンポーネントや情報漏洩防止、電子署名・認証、セキュア B2B などの各ソリューションを活用して、顧客ニーズにフィットした業務システムを迅速に構築するセキュリティ応用ソリューションを提供する。

1. まえがき

インターネットの普及、ハードウェアの高性能化と低価格化、J2EE (Java2 Enterprise Edition) に代表される Java 仕様の成熟化などにより、急速な Web 技術の普及が進んでいる。“企業グループ全体での最適化”、“プロセス統合による業務改善”、“汎用機からのリプレース”など企業内の大規模な基幹系システムの再構築でも積極的に Web 技術が採用されつつある。政府においても経済産業省が高度な電子政府システム実現のために発足させた“IT アソシエイト協議会”の中間報告の中で、Web アプリケーションを中心としたモデルがまとめられている。

MDIS では得意とする情報セキュリティ技術と Web 技術の体系化を進めている。本稿ではこのセキュア Web ソリューション体系の構成要素について述べ、その中のセキュリティ応用ソリューションの事例を紹介する。

2. セキュア Web ソリューション

2.1 背景

Web ベースのシステムには多くのメリットが挙げられる。

- (1) ネットワーク型システムに適している。
- (2) ミドルウェアやプラットフォームの依存度が低い。
- (3) 拡張性が高い (技術革新の余地が大きい)。
- (4) オブジェクト指向開発に適しており、生産性・保守性の向上が期待できる。
- (5) クライアントにプログラムを配布する必要がなく運用管理が容易である。
- (6) インターネットを容易に活用できる。

これらのメリットがある反面、セキュリティ上のリスクも多く、実際に“不正アクセス”、“データ改ざん”、“データ流出”などのセキュリティ関連事故が数多く報告されている。また、ネットワーク化の進展や電子メールの普及、多様化する雇用形態などの社会環境の変化に伴って個人情報保護法成立や不正競争防止法改正など法整備が進められていることや、セキュリティ事故によるリスクが現実の問題として認識されるようになってきたことから、情報セキュリティへの関心は高まってきている。

このようなニーズに応えるために、セキュリティ技術を活用したトータルな Web インテグレーションフレームワークを、セキュア Web ソリューションとして体系化した。このソリューションを提供することにより、以下のようなメリットを生み出し、IT による企業の業務革新を安全・安心なシステムで実現することを可能とする。

- (1) セキュリティを考慮した共通セキュアコンポーネントを再利用することで、セキュリティの高いシステムを効率的に構築。
- (2) 暗号、署名・認証などのライブラリを活用して高度なセキュリティ機能を実装。
- (3) 文書管理や B2B などのソリューションにセキュリティ機能を組み込むことで新たな付加価値を創出。

2.2 セキュア Web ソリューションの構成

セキュア Web ソリューションは図 1 に示すように大きく 3 つのパートから構成されている。

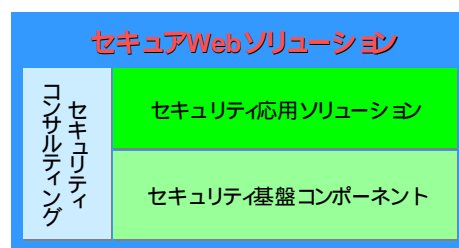


図 1. セキュア Web ソリューション構成図

それぞれの詳細は次のとおりである。

2.2.1 セキュリティ基盤コンポーネント

セキュリティ基盤コンポーネントはセキュアなシステムを構築するための文字通り基盤をなすコンポーネント群である。単体でセキュリティ機能を実現している暗号や PKI を応用したソフトウェア製品、システム (アプリケーション) にセキュリティ機能を実装するためのライブラリ製品、セキュアなシステムの構築に利用できる共通セキュアコンポーネントで構成される (図 2)。

それぞれのコンポーネントは PKI 技術や暗号アルゴリズム MISTY^(注1)をはじめとした三菱電機グループのセキュリティ技術を活用した特長的なソフトウェアである。システム構築に必要なソフトウェア上のセキュリティを“共通セキュアコンポーネント (Java コンポーネント)”としてまとめ、再利用することでシステム構築における生産性を高めることができる。



図 2. セキュリティ基盤コンポーネント

2.2.2 セキュリティ応用ソリューション

セキュリティ応用ソリューションは、要旨イメージ図に示したように、セキュリティ基盤コンポーネントと、企業や官公庁・自治体における情報の漏洩を防ぐための情報漏洩防止ソリューション、電子文書を安全に扱うための電子署名・認証ソリューション及び企業間のセキュアなデータ交換を行うためのセキュア B2B ソリューションなどを活用して高度な情報セキュリティシステムを構築するためのソリューションである。また、各種業務システムの構築ノウハウをテンプレートとして蓄積しているので、顧客ニーズ

(注 1) MISTY、CRYPTOFILE、CryptoSign、TRUSTWEB、PowerMISTY、CERTMANAGER、CertMISTY は、三菱電機(株)の登録商標である。

(注 2) DROSY、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。

にフィットしたシステム化を短期間に構築できる。

2.2.3 セキュリティコンサルティング

セキュリティコンサルティングは企業や官公庁・自治体などの情報セキュリティシステムを人的・物理的な側面も含めて構築するコンサルティングサービスであり、現在は次の4つのサービスメニューを用意している。

(1) ISMS 認定取得支援 (ISMS 構築運用支援サービス)

これまで企業などの組織におけるセキュリティは外部の脅威への対策がクローズアップされていたが、社会的な環境変化やネットワーク化の発達などにより、内部の脅威への対策も重要視されてきた。これらのセキュリティを総合的・体系的に管理することが組織の安全と信用に不可欠であることから、ISMS (情報システムマネジメントシステム) の導入が盛んになっている。

このようなニーズに対し、“ISMS 構築・運用の支援”及び“ISMS 適合性評価制度に基づく認定取得の支援”を行うコンサルティングサービスを用意している。認定取得の実績も多数あり、豊富な実績をもとにコンサルティングを提供している (図3)。

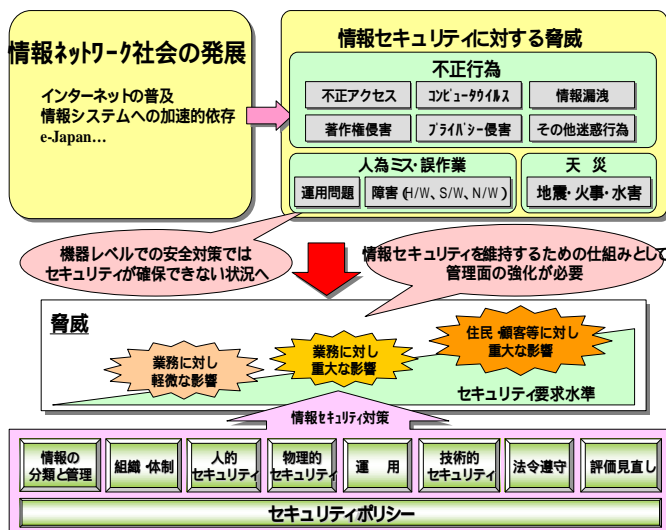


図3. ISMS 構築運用支援サービスのイメージ図

(2) セキュリティリティ診断 (情報セキュリティベンチマークサービス)

ISO17799 等の国際基準に適合しており、セキュリティポリシー、物理的セキュリティから運用管理のセキュリティまで、10種のセキュリティ領域をカバーしたベンチマーク分析を実施している。企業における情報セキュリティ投資のレベルを判断する材料として利用することができ、定量的な他社との比較を行うこともできる。

(3) セキュリティポリシー策定 (セキュリティポリシー・ベストプラクティスパッケージ)

企業や官公庁・自治体向けのセキュリティポリシー策定をサービスメニューとして用意している。LGWAN (Local Government Wide Area Network: 総合行政ネットワーク) にも対応しており、実績をもとにした具体例及びサンプル文書を提示し、運用・保守性の高い情報セキュリティ

ポリシー策定を支援する。

(4) 認証局運用規定 CP/CPS 策定 (特定認証業務認定取得支援サービス)

このサービスは、電子署名法で定める認証業務を行う認証局の構築に必要な証明書のポリシー及び認証局の運用規定の作成支援をするものである。認証局構築の実績に基づいた、“業務設計”、“トラステッドロール提案”及び“審査基準提案”を行いながら、認証局としての CP 及び CPS の作成を支援する。

3. システム事例

3.1 電子帳票配信サービス

セキュリティ応用ソリューションのシステム事例として、三菱電機情報ネットワーク(株) (MIND) 向けに MDIS が構築した“電子帳票配信サービス”がある (図4)。これは MIND が展開している EDI サービスの付加価値サービスの一つであり、MDIS の企業間電子商取引システム < EDIFOAS/B2B (注3) > と電子署名ソフトウェア < SignedPDF > を活用し、帳票配信テンプレートを使って短期間に構築した (2004年サービス開始予定)。

これまでの EDI は発注・仕入・請求など取引データの送受信をオンライン化することで業務を効率化していたが、実業務では依然として請求書や帳票などのビジネスドキュメントが紙で存在している。電子帳票配信サービスはこれらビジネスドキュメントの発送など、ハンドリングを含めた業務の効率化を実現することができる。取引によって発生する請求書や帳票などのビジネスドキュメントは PDF ファイルとして電子帳票化し、電子署名によって文書の真正性を確保することで、安心・安価・確実・迅速に配信することが可能となる。

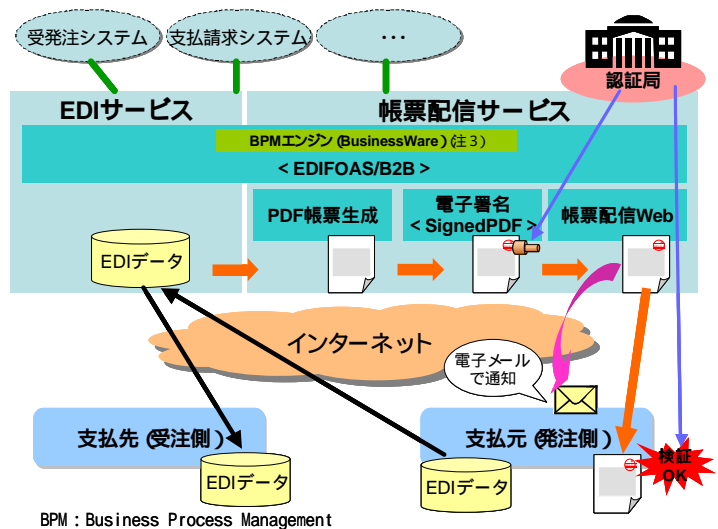


図4. MIND の電子帳票配信サービスイメージ図

例えば、EDI によって受信した受注データを利用して、締め日ごとに請求書を電子署名付 PDF で生成する。請求書が配信可能になったことを支元元 (発注側) に電子メールで通知し、支元元は Web を利用して請求書をダウンロードす

(注3) EDIFOAS/B2B は、三菱電機(株)の登録商標である。

(注4) BusinessWare、VITRIA は、米国 Vitria Technology, Inc. の登録商標である。

る。ダウンロードデータはHTTPS (Hyper Text Transfer Protocol Security) によって暗号化されているため盗聴される心配はなく、請求書自身も電子証明書を使用した電子署名によって真正性を確認できる。また、支払先(受注側)もWebによって請求書のダウンロード状況を確認することができる。電子帳票はユーザ・フォーマットごとに対応し、支払い通知や買掛一覧などEDIに関連する帳票配信をサービスとして提供する。

<EDIFOAS/B2B>にはBPM(Business Process Management)エンジンとしてVITRIA(注4)社のBusinessWareが組み込まれているため、EDIを中心に様々な付加価値サービスを拡張することができる。また、eXML(electronic business eXtensible Markup Language)やWebサービスにも対応することによってサービスの幅を広げていく予定である。

3.2 共有文書機密管理システム

情報漏洩防止を目的としたセキュリティ応用ソリューションのシステム事例として、MDISが某製造業向けに構築した共有文書機密管理システムがある。このシステムは、社内共有文書の閲覧を許可された利用者だけに限定するもので、情報漏洩防止ソリューションのコンポーネントの一つである三菱電機利用権管理ソリューション<DROSY>を活用して構築した。

<DROSY>は、DRM(Digital Rights Management)技術を応用した再配布コンテンツのセキュリティを確保するためのソリューションで、PDFやMicrosoft(注5)Office文書を暗号化し、認証された利用者だけにライセンス(復号鍵+利用情報)を配布して暗号化した文書の閲覧を可能とする。ライセンスは、利用者ごとにパーソナライズ(個別化)しているため、万が一、他の利用者がこのライセンスを不正に入手したとしても利用することはできない。暗号化した文書はメモリ上でのみ復号し、平文を作らないことにより不用意な情報の漏洩を防ぐ。また、利用者の閲覧権限は回数、期間などで限定できるので、様々な利用形態に適應できる。<DROSY>のサーバ側ソフトウェアはJ2EEでつくられており、ユーザインターフェース及び外部システムインターフェースもすべてWebベースにしている。

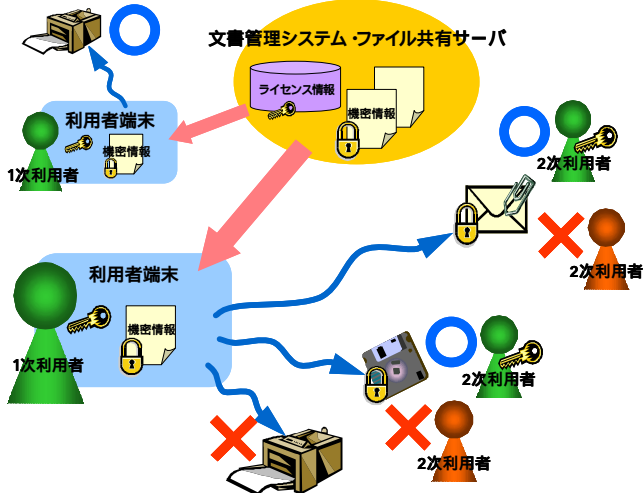


図5. <DROSY>の利用権管理機能

従来、文書管理システムなどで文書のセキュリティを確保するためには、オペレーティングシステムやソフトウェアのファイルアクセス制御機能を使っていたが、この<DROSY>を活用することで文書管理システムなどから文書を取り出した後も常にユーザの利用権限をチェックすることができ、万が一、故意・過失によって文書ファイルが流出した場合でも内容の漏洩を阻止することができる。

<DROSY>は、すでに文書管理システムが導入されているユーザにも容易に導入することができる。例えば、共有文書をPDF化する業務フローに<DROSY>で暗号化する処理を追加することで、共有するPDF文書に利用制限を設定することができる。また、文書管理システムで利用者認証にLDAP(Light weight Directory Access Protocol)サーバを利用している場合、<DROSY>もこれを利用して文書管理システムのアクセス権をそのまま引き継ぐことが可能である。これにより、文書セキュリティシステムを導入した後もユーザは従来の処理フローと変わりなく、文書を利用することができる。万が一、ユーザが手元にダウンロードしたPDF文書が媒体や電子メールで外部に流出しても、文書管理システムにおいて利用者の閲覧権限を確認しなければそのPDF文書を開くことはできない(図6)。

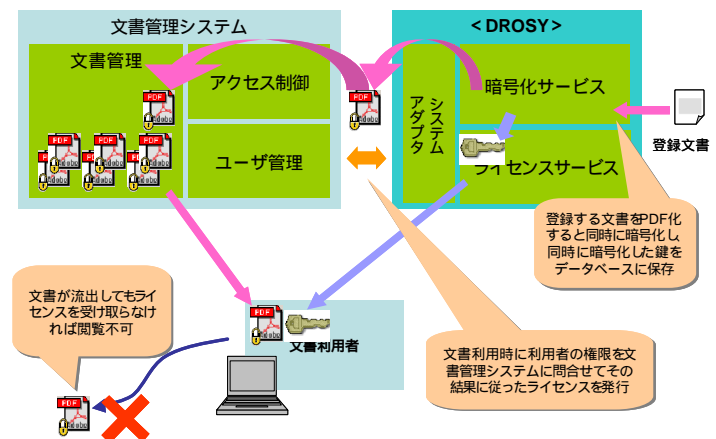


図6. 共通文書機密管理システムの事例

機密情報の共有において、これまではセキュリティの観点から共有する範囲を限定していたケースでも、<DROSY>を導入することによりセキュアな情報共有が可能になり、セキュリティの確保と生産性向上の両立を図ることができる。

4. むすび

今後、システムのWebベース化や業務システムでのインターネット利用の拡大、Webサービスの普及などによって、これまで以上に情報システムにおけるセキュリティの確保が必要になる。この意味でもSIベンダーとしては、安全で安心なソリューションを確実に提供することがますます重要になってくる。進化する環境とニーズに応じて、セキュアWebソリューションをより一層充実させ、安全・安心と利便性を両立させた情報システムソリューションを提供していく所存である。

(注5)Microsoftは、米国Microsoft Corp.の米国及びその他の国における商標又は登録商標である。