導入が簡単で安心な中堅企業向け情報漏洩防止ソリューション

Solution for Information Leak Protection of Small- and Medium- sized Enterprises

森口　隆史*
(Takashi Moriguchi)
中村　稔*
(Minoru Nakamura)
岡本　忍*
(Shinobu Okamoto)

要　旨

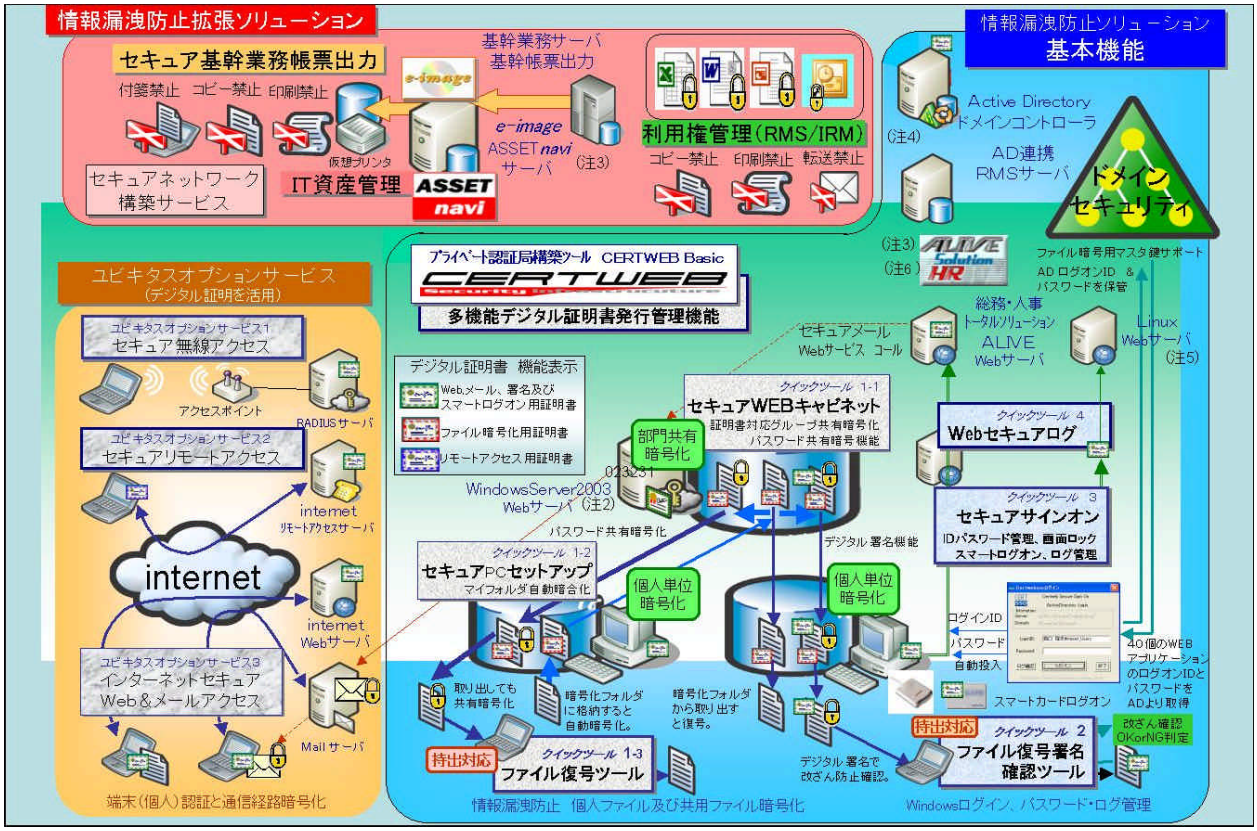
個人情報保護法が2005年4月より本格施行され，情報漏洩防止が急務となっている。中堅企業の情報システム構築においては，短期で安価なシステムの開発及びシステム変更に対する柔軟性等が特に要求され，システムの柔構造が必要という特徴を有している。一方で，個人情報保護対策に関しては，企業の規模に関係なく要件は同じであり，中堅企業ならではの工夫を凝らした情報漏洩防止のソリューション技術が必要となる。

㈱三菱電機ビジネスシステム(MB)では，独自のプライベート認証局構築ツール“CERTWEB(注1)”と，マイクロソフト社のWindows(注2)ディレクトリ管理機能を組み合わせることにより，強固なセキュリティマネジメントを実現する情報漏洩防止ソリューションを開発した。

情報漏洩防止等のセキュリティ対策においては，どこかに対策漏れがあれば元も子もなくなり，バランスのとれたシステム構築が重要となる。本ソリューションは，企業内をドメインセキュリティで対策し，企業外の無線LANやインターネット接続はユビキタスセキュリティで対策する点が特長であり，一貫したシステム構築をワンストップで提供する。

本稿では，中堅企業に焦点を当てた情報漏洩防止ソリューションの構築技術について記述し，中堅企業向けにMBが新たに開発した“導入が簡単”で“安心頂ける”情報漏洩防止ソリューションを紹介する。

(注1) CERTWEBは，㈱三菱電機ビジネスシステムの登録商標である。
(注2) Microsoft, Windows, Windows NT, Windows Server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 3) ALIVE Solution, e-image, ASSETnavi は，㈱三菱電機ビジネスシステムの登録商標で ある。
(注4) RMS(Windows Rights Management Service), IRM(Information Rights Management), AD(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。
(注5) LinuxはLinus Torvalds の米国及びその他の国における登録商標又は商標である。
(注6) HRは、Human Resourceの略語である。

中堅企業向け情報漏洩防止ソリューションの概念図

Active Directoryのコンサルティングと，MBが提供するプライベート認証局CERTWEBが発行する多機能デジタル証明書を中核として構成している。最小限度必要な暗号化機能をオールインワンで提供し，シンプルで手間がかからずに早期導入できる中堅企業向けの情報漏洩防止ソリューションである。オプション機能として，即活用できるクイックツールが用意されており，想定された用途に簡単に拡張できるユビキタスオプション構築サービスが用意されている。セキュア基幹業務帳票出力やIT資産管理等の拡張ソリューションもある。

*㈱三菱電機ビジネスシステム

1．ま え が き

個人情報保護法が2005年4月より本格施行され，情報漏洩防止が急務となっている。中堅企業の情報システム構築においては，短期で安価なシステムの開発及びシステム変更に対する柔軟性等が特に要求され，システムの柔構造が必要という特徴を有している。

一方で，個人情報保護対策に関しては，企業の規模に関係なく要件は同じであり，中堅企業ならではの工夫を凝らした情報漏洩防止のための要素技術が必要となる。

本稿では，情報漏洩防止に関する個別のセキュリティ対策から，ディレクトリ管理／ネットワーク構築におけるセキュリティ対策，個人認証／アクセス制御，さらには運用監視等のサポート＆サービスまで含めて，一貫した個人情報漏洩防止ソリューションを提供するための構築技術を紹介する。

2．中堅企業向け情報漏洩防止ソリュ－ションに求められるものとは

通常，情報セキュリティマネジメントシステム(ISMS)構築は，実践可能なセキュリティポリシーを確立し，運用管理するのが基本である。運用だけでは実現できない要素技術については，何らかの対策が必要となる。即効果の出る暗号化の導入によりまず現状防衛を行いつつ，トップダウンで本格的なセキュリティポリシー，情報漏洩防止ポリシーを構築し実践していく方法が，中堅企業でのベストプラクティス(現実的最良策)として採用されているケースが多い。

2.1 個人情報保護法対応の必要性

個人情報保護法対応した情報漏洩防止対策を行うには，各省庁から出ている実施ガイドラインに準拠した対応（組織的，人的，物理的，技術的安全管理措置）が必要となる。また技術進歩に応じた継続的見直しも必要であり，技術的に実現不可能な内容は運用管理で対応する必要がある。

具体的には，ISMS適合性評価制度による認定を取得するのが望ましいが，人材確保や費用面の問題もあり，中堅企業では，プライバシーマーク(Pマーク)の取得を現実的な対応としてまず採用する場合が多い。今後，Pマークあるいは ISMSの取得がないと，受注(入札)もできなくなるケースが増えてくると予想される。

2.2 中堅企業ならではの工夫が必要

しかしながら，中堅企業へのアンケート結果では情報漏洩防止の方法としては，“保険と教育”との回答が多く寄せられ，対応内容に対する認識のズレが大きい。また，情報技術(IT)を活用した情報漏洩防止の方法についても，要求仕様を比較的小規模の人員で効率よく実現できることが求められている。

3．バランスのとれたコストパフォーマンスの実現

情報漏洩防止を効率よく実現するには，早期のシステム稼働，システム変更に対する柔軟性等が特に求められるが，さらに，セキュリティ対策漏れがないバランスのとれた対応も重要である。

3.1 システム柔構造の提供

セキュリティシステムを導入すると，維持管理に手間がかかり，IT化に伴う運営費用TCO(Total Cost of Ownership)も増加する傾向がある。したがって，スモールスタートが可能で，段階的に拡張できる柔軟なシステム構造が必要となる。

導入し易く，かつ拡張性を確保するために，MBではマイクロソフト社のWindowsのディレクトリ管理機能，アクセス制御技術をシステム構築ツールとしてパッケージ化することで，段階的な導入とシステム信頼性を確保している。

3.2 ユビキタス時代の一貫したシステム構築支援技術

ブロードバンドの高速・低価格化と，モバイルパソコン，PDA(Personal Digital Assistant)等の省電力高性能化により，ユビキタス社会が加速されている。ユビキタス社会の進展に伴い，社内接続セキュリティの重要度も増しているが，一方で，高度なIT化に対応できる専任管理者が不在という中堅企業独特の問題点もクローズアップされつつある。

これらに対応するため，MBではセキュアなディレクトリ構築，ネットワークセキュリティ構築から，運用監視サポート＆サービスまで行う一貫したシステム構築・運用支援サービスを含む情報漏洩防止ソリューションを提供している。

4．中堅企業向け情報漏洩防止ソリュ－ション

今回開発したソリューションのねらいは，シンプルな管理で手間がかからず早期に導入を可能とすることである。プライベート認証局の構築支援ツールであるCERTWEBから発行される多機能デジタル証明書は，最小限度必要なセキュリティ機能をオールインワンで提供している。このオプション機能には，即活用できるクイックツールが用意されており，想定される用途を簡単に拡張できるユビキタスオプションの構築サービスも提供している。

4.1 核となるデイレクトリ管理

情報漏洩防止のコア技術として，AD (Active Directory)構築技術を位置付けている。

Windows NT Sever のドメインやワークグループ等のサーバごとにユーザ情報が散在している場合には，“どこの誰”ということが一意に決まらないため，アクセス制御も非常に難しくなる。ADによるディレクトリ管理の基本は，既存の環境をシングルドメインに集約することである。

ADの導入では，GPO(Group Policy Object)の応用による管理コストの低減や，AD連携を前提としたWindows利用権

管理等の新機能RMS(Rights Management Service)及びIRM(Information Rights Management)が活用できるというメリットもある。

4.2 オールインワンの暗号化環境

アクセス制御はオペレーティングシステム(OS)が提供している機能であり,ハードディスクを取り出されてしまっては効果が無い。そこでOSのアクセス権にプラスしてファイル暗号化も必要となる。機密情報暗号化については,各省庁等のガイドラインに安全管理措置が明記されている。Pマーク制度でもその監査ガイドライン(JIS Q15001準拠)「個人情報利用の安全性の確保」に,「情報システム安全対策基準」や「コンピュータ不正アクセス対策基準」を参考にした安全対策を必要とすると明記されており,その情報漏洩防止機能として,暗号化する機能を設けることとされている。

(1)暗号による管理策について

ISMS評価制度の原典であるJIS X5080:2002の「暗号による管理策について」の中に,暗号使用についての個別方針を定め,組織全体で暗号による管理策を用いることへの管理層も含めた取り組みが必要であると記載されている。また,鍵の紛失や損傷またそのセキュリティが脅かされた場合の情報回復手段も取り決めておくこととしている。

マスタ鍵管理や情報回復策,暗号化メール等はその履歴を一定期間保管しておく等の暗号化自体の管理策も具体的に準備しておく必要がある。基本的には,極秘情報については,メールやファイル転送等の手段を用いないといった個別方針も存在するが,暗号化した形態で通信やメールの実施という管理策も考えられ,特にインターネットでは有効な対策となる。

(2)通信経路暗号化と電子メール暗号化

MBではインターネットにおける暗号化を，CERTWEBが発行するデジタル証明書により実現している。

さらに,この機能をイントラネットに展開する場合,MBが開発した人事・総務部門向け最新ソリューションであるALIVE Solutionに対しては,CERTWEBを組み合わせたセキュアALIVE Solutionとして SecureSignOn, SSL(Secure Socket Layer), S/MIME(Secure/Multipurpose Internet Mail Extensions)による業務セキュリティを提供している。

SecureSignOnはシングルサインオンとしても機能し,先の「コンピュータ不正アクセス対策基準」でのパスワード及びユーザーID管理を支援する。

SSLでは,サーバ証明書によりWeb通信経路上のID,パスワード等,通信データ保護を行う。

また,管理者画面は,特定のクライアント証明書を持つ管理者のみがアクセスできる形態を実現している。

S/MIMEは,ALIVE Solutionの機能であるインターネットによる給与支給明細の自動配信でメールの暗号化を実現している。

(3)端末とサーバのファイル暗号化

CERTWEBは,Windowsの暗号化ファイルシステム(EFS)とスタンドアロン型のMicrosoft Certificate Serverを活用して,暗号化環境及びプライベート認証局をオールインワンのシンプルな形態で提供する機能を有している。CERTWEBのオプション機能では，HTTPS(Hypertext Transfer Protocol Security)によるファイル暗号送受信機能とサーバ側フォルダの部門単位共有暗号化機能，Windows2000以降のクライアントでワンタッチでマイフォルダの暗号化を行う機能等も実現した。さらに同一ドメイン内にログインするクライアントの暗号化は,共通のマスタ鍵での復号も可能としている。ただし，マスタ鍵は一般には使用できないよう厳重保管を行い,監査等で使用する際にも鍵管理者立会いで対応する等の運用ルールの取り決めを薦めている。

CERTWEBのオプション機能には情報管理台帳機能もあり，情報に機密区分（機密情報,個人情報,極秘）を設定して状態（入力[取得],持出[利用],戻し[保管],廃棄等）フェーズを管理できる。この機能は,ドメインにログオンしたユーザーは暗号化を意識せずに利用できるが,暗号化フォルダからファイルを持ち出すと暗号は解除されてしまう。そこで,機密区分が極秘の場合は乱数パスワードによる明示的な暗号化を自動的に行なう機能を有し,これによりどこに持ち出しても暗号化され,このファイルの復号には専用復号ツールとそのパスワードが必要になる。

さらに“PowerMISTY(注7)”による改ざん防止署名暗号化と署名確認復号ツールも提供している。

また，CERTWEBオプション機能の不正アクセス防止機能としては,スマートカードログイン機能とログインログ及び離席画面ロック機能を有している。

これらの個人情報を含む機密情報の管理支援機能で,中堅企業の兼務管理者の負担を軽減し,ユーザーセキュリティの向上を図っている。

5．ユビキタス環境における情報漏洩防止対策

一方,2005～2010年のu-Japan構想で,さらに加速するであろうユビキタス環境にそなえたセキュリティ対策として,CERTWEBのデジタル証明書を活用した高度なユビキタスセキュリティを構築するオプションサービスを用意している。

5.1 インターネット対応の暗号化を含むアクセス制御

ひとつは,出張先や自宅から社内へのリモートアクセスを,端末証明書によるインターネットVPN接続で実現するサービスである。これにより従来のセキュアなWeb接続だけ

（注7）PowerMISTYは，三菱電機(株)の登録商標である。

でなく,クライアントサーバ接続でもセキュアな環境を実現できる。

5.2 イントラネット対応の暗号化を含むアクセス制御

もうひとつは,社内無線LAN接続のウィークポイントである通信経路暗号化を行い,さらに証明書を格納した端末のみ社内LANに暗号化接続できる環境を提供するサービスである。これにより社内クライアントのみ社内LANに接続できる無線LAN環境を構築できる。

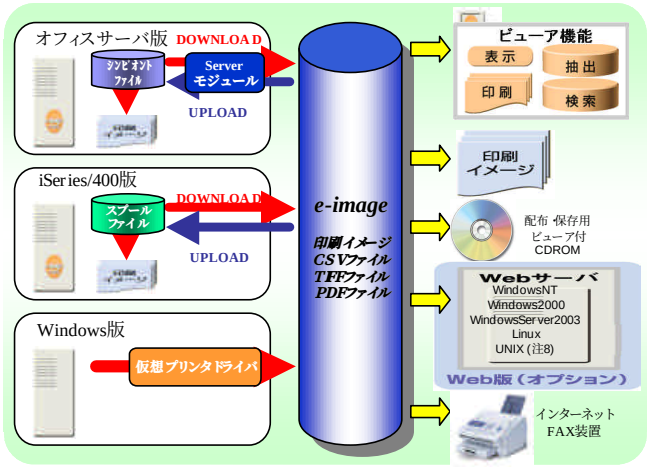
6．中堅企業向け情報漏洩防止 拡張ソリューション

情報漏洩防止ソリューションを支える拡張ソリューションについて以下に紹介する。

6.1 基幹業務帳票セキュア出力

電子帳票帳票システムe-imageのセキュアオプション機能では,基幹業務からの帳票出力を電子ファイル化し,そのデータの利用権管理を実現している。

e-imageはオフィスサーバ版,IBM eServer(注９) iSeries 400版, Windows版があり,簡便に電子帳票へのアクセス制御を実現している(図１)。



コンピュータの“印刷データ”を取り込んで、ペーパーレス、データの有効活用・再利用、電子帳簿保存法への対応を実現するソフトウェアツール

図１．e-image概要図

e-imageでは,専用ビューアを使用するユーザーまたは組織毎に,帳票又は帳票グループのアクセス権を設定できる。アクセス権には,以下の種別がある。また,参照権限がない帳票は,その存在も見せないセキュリティとなる。

(１)全ての操作が可能　　(２)参照操作が可能
(３)印刷操作が可能　　(４)付箋の参照が可能
(５)付箋の書き込みが可能
(６)エクスポートが可能（クリップボードへのコピー,PDF変換,HTML変換）

ユーザーと組織の設定には,以下のひとつが選択できる。

(１)WindowsのADのユーザ情報を使用する。
(２)Windowsのドメインユーザのユーザ情報を使用する。
(３)e-image独自にユーザ情報を設定する。

参照・印刷履歴機能により,帳票毎に,参照と印刷の履歴（何時・誰が・何を）を管理できる。この履歴はビューアの帳票プロパティから参照できる。

6.2 IT資産管理

情報漏洩防止に関連し,不正な端末の接続や不正ライセンスの使用を監視するIT資産の管理も合わせて実施することが望まれる。IT資産管理システムASSETnaviは，これらを直感的に簡単に管理できるツールとして提供している。

6.3 セキュアネットワーク構築

上記ソリューションを支えるインフラ構築サービスとして，セキュアネットワーク構築サービスがある。

(1)セキュアネットワークとは

以下の要件を実現するネットワークである。

・接続許可の人（クライアント）しかアクセスできない
・使いたい時に使える（ダウンしない）
・障害発生時にその詳細状況を管理者が把握できる
・障害原因の追求が行える
・不要なトラフィックを発生させない
・ウィルスが蔓延しない

(2)セキュアネットワーク実現策

セキュアネットワーク構築サービスでは，認証・攻撃防御・冗長・証拠・障害検知・脆弱性の各側面からの対策を実施する。“認証”は無線LANに認証VLANを構築し,ログインID単位のアクセス制御方式を実現する。“攻撃防御”はファイヤウォール／不正侵入検知防御装置(IDP),“冗長”は基幹スイッチおよび経路の冗長化やインターネット接続回線の冗長化・負荷分散,インターネットVPN環境の冗長化をサポートする。“証拠”はフォレンジックサーバ,“障害検知”は内部のスイッチをSNMP(Simple Network Management Protocol)で一括管理する。“脆弱性”は,インターネットやサーバネットワークにパッチやウイルスパターン未更新等の危険なクライアントパソコンを接続させない検疫ネットワーク構築等に対応している。

7．む　す　び

中堅企業にフォーカスした情報漏洩防止を効率よく実現することは，情報システム進展の加速・高度化のために，今後ますます重要となってくる。

より便利で安心･安全な最新情報漏洩防止ソリューションを今後とも提供していく所存である。

参　考　文　献

(1)個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン 平成16年10月 ,経済産業省（2004）

（注８）UNIXは，The Open Groupがライセンスしている米国ならびに他の国における登録商標である。
（注９）IBM, eServerは，IBM Corp.の商標である。