

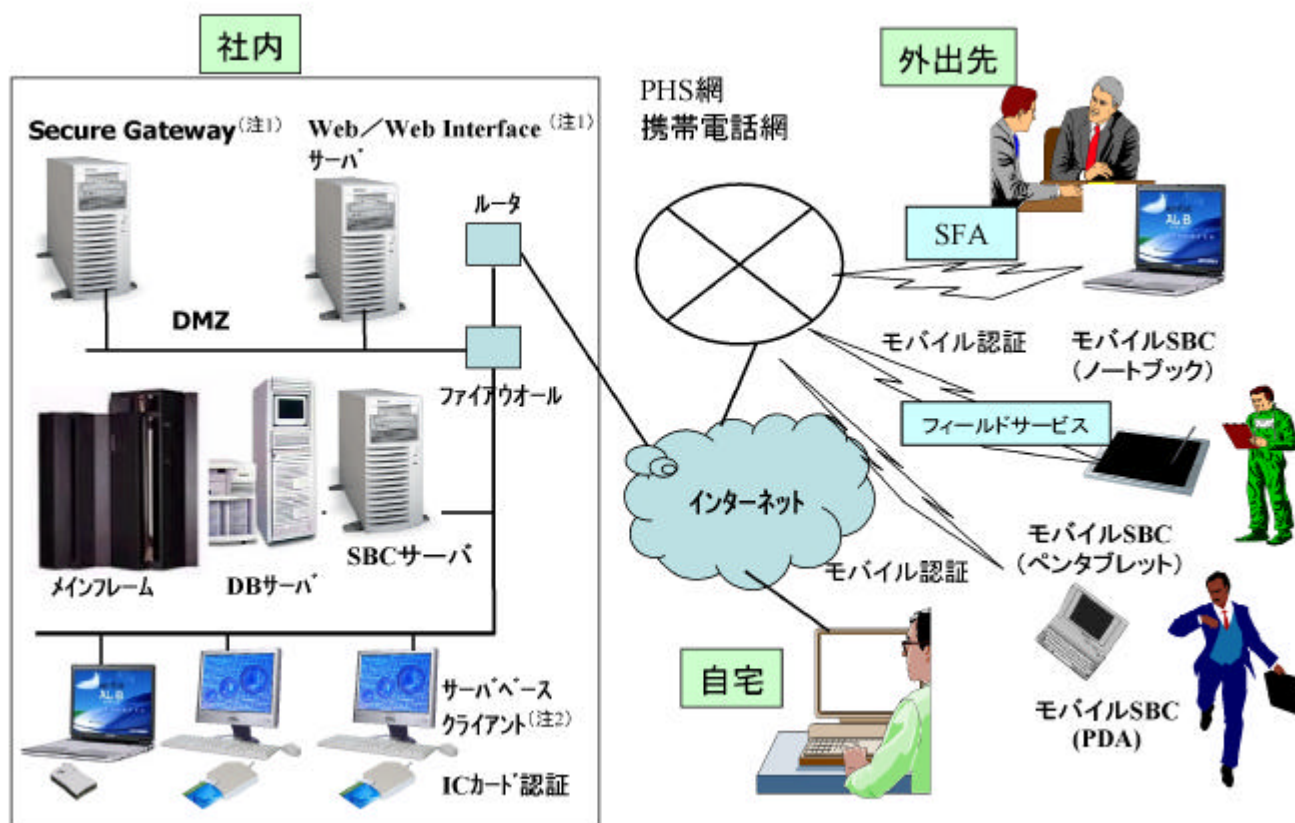
要 旨

安全な情報システムでは、機密性、完全性、可用性が求められる。情報システムのセキュリティ技術は、暗号技術や個人認証技術によりネットワーク上での盗聴、データ改ざん、なりすまし、不法侵入、データ破壊等の意図的な脅威から守ってくれる。但し、セキュリティを保つためには、過失、故障、災害等の偶発的な脅威に対しても対策する必要があり、技術面だけでなく、人的対策としてのユーザ教育、モラルの徹底、制度的な対応として手順書等による運用面での徹底、H/Wの故障や地震、火災等の脅威に対して建物や設備に対する対策が必要である。これらを対策するためには、バランスのとれたセキュリティシステムを構築する必要がある。

特に、ユーザ教育やモラルの徹底等の人的対策や運用面での対策に頼るセキュリティに対しては、技術面でのセキュリティ向上が求められている。三菱電機インフォメーションテクノロジー(株)(MDIT)では、ソフトウェア、データを全てサーバで管理する“サーバベースコンピューティング(SBC)ソリューション”により、運用や人的なセキュリティ上の脆弱さを技術的な仕組みとして対策し、いつでもどこでも安心して、オフィスと同じ環境にアクセスできる、トータルなセキュリティソリューションを提供している。

(注1) Secure Gateway、Web Interface は、米国 CITRIX社の登録商標である。

(注2) サーバベースクライアントは、三菱電機インフォメーションテクノロジー(株)の登録商標である。



DMZ : DeMilitarized Zone
DB : Data Base
SFA : Sales Force Automation
SBC : Server Based Computing
PDA : Personal Digital Assistant

SBC トータルソリューション

ユビキタス社会への期待が高まっている中で、社内・外出先・自宅などから、いつでもどこでも、多様な通信サービス等を利用して、センターのSBCサーバに接続することにより、オフィスと同じ環境を安心して使えるためのトータルソリューション(端末ソリューション、認証ソリューション、設計・構築ソリューション)が“SBC トータルソリューション”である。図中の Secure Gateway と Web Interface は、クライアントから Web ブラウザを利用して、安全に SBC サーバに接続するためのユーザ認証と暗号化を行うためのサーバである。

1. まえがき

企業での情報漏洩の大部分は、内部からの漏洩であると言われており、人的なセキュリティ対策を如何にして技術的な仕組みとして取り込めるかがセキュリティ対策上の大きな課題である。本稿では、SBCにより技術的な仕組みとして、人的なセキュリティを強化し、いつでもどこでもオフィスと同じ操作環境を提供するセキュアなSBCセキュリティソリューションについて述べる。

2. 情報システム・セキュリティでの問題点

(1) セキュリティの重要性

企業において情報発信、情報収集、情報交換、ビジネス等にインターネットは無くてはならない存在となってきた。インターネットゆえに、世界中のハッカーから通信データの盗聴、改ざん、システムの破壊等の危険に常時さらされている。また、2003年8月に猛威を振るったMS Blasterウイルスは、史上最大規模の被害を与え、ウイルス問題は後を絶たない。さらに、個人情報漏洩に関する事件が多発しており、こうした被害から自社システムを守り社会への信用を得るために、情報システムのセキュリティ対策の重要性は言うまでもない。

(2) セキュリティ対策

安全な情報システムでは、機密性(盗まれない)、完全性(壊されない)、可用性(いつでも使える)が求められる。こうしたシステムの対策としては、代表的なリスクの原因からアプローチする方法として以下の対策が必要である。(a) 技術的対策としては、ネットワークセキュリティ対策が重要な要素であり、暗号と認証技術によりネットワークでのデータ破壊、改ざん、盗聴、不正アクセス、なりすまし等からセキュリティを保つ。(b) 物理的セキュリティ対策としては、重要な情報資産を厳格な入退出管理を伴った耐震構造建物などに設置するなどの対策やIDC(Internet Data Center)でのバックアップ等により各種被害・災害等から守る。(c) 人的セキュリティ対策としては、セキュリティ教育、モラルの向上、運用規約などにより、人的不注意によるデータ漏洩を防ぐ。

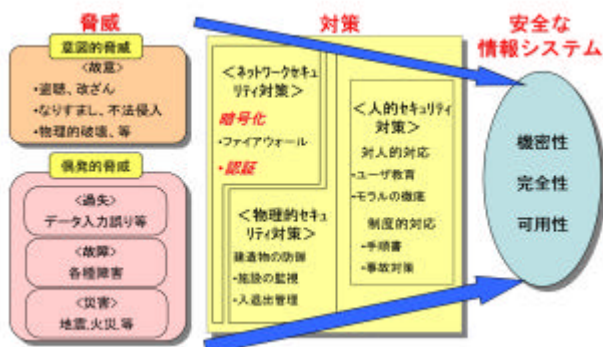


図1. 安全な情報システムのためのセキュリティ対策

(3) 人的セキュリティ対策の重要性と課題

企業における情報漏洩の大部分は、内部の人的ミスや故意によるものと言われており、人的なセキュリティ対策部分をモラルや人の運用のみに頼るのでなく技術的な仕組みでセキュリティを向上することが大きな課題となっている。

3. SBCでのセキュリティとは

(1) SBC方式の背景

情報システムの構築方式として、1990年代に入りホスト集中システムから、安価なサーバでシステムを構築できるクライアント/サーバシステム(C/Sシステム)に移行を開始した。1990年代後半からは、クライアント台数が増えることによる管理コストの増大とクライアント側のセキュリティ強化の面から、新たなサーバ集中方式としてインターネットとの親和性の高いWebシステムへの移行が進みつつある。しかしながら、C/SシステムからWebシステムへの移行は、システムの再構築が必要であり、多大な開発投資を必要とする。そこで、既存のC/Sシステムをそのまま利用して全ての業務をサーバで集中管理可能なSBCシステムが注目を浴びている。

(2) SBC方式の仕組み

C/Sシステムのクライアントとサーバの間に、SBCサーバを置き、クライアント側にあったアプリケーションとデータ全てをSBCサーバ上に置いて動作させる。クライアントとSBCサーバの間では、画面情報とキーボード、マウス等の情報だけが交換される。クライアント側では、画面を制御するSBCクライアントソフトウェアが動作するだけで、あたかも、端末でWindows(注3)が動作しているようにみえる。サーバ側では、複数のクライアントからの要求を受け付け、端末対応に論理的な仮想端末を生成し、各々が独立した端末として動作するよう制御する。これにより、システム独自のアプリケーションだけでなく、Excel(注3)、Word(注3)、Outlook(注3)等のOA系のアプリケーションも全てサーバでの集中管理が可能となる。

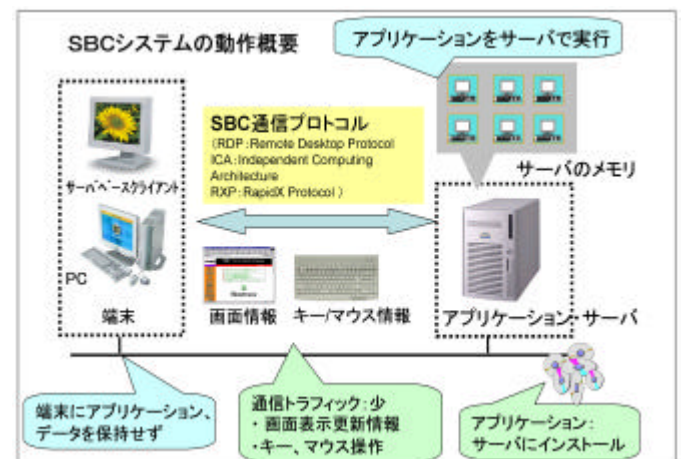


図2. SBCシステムの動作概要

(注3) Windows、Word、Excel、Outlook、Office は、米国 Microsoft 社の登録商標である。

(3) セキュリティに関する特長と効果

これまでの人的なセキュリティ対策は、従業員の教育、モラル、運用等に頼ってきたが、SBC では技術的な仕組みとして、以下のようなセキュリティを確保できる。

(a) 情報の不正持ち出し防止

データを全てサーバで管理し、端末側ではサーバの仮想端末の画面表示が行われ、また端末のデータ入出力はサーバ側で制限をかけることが可能なので、端末を通じた情報の不正持ち出しを技術的な仕組みとして防止できる。

(b) モバイル端末盗難紛失時のセキュリティ

モバイル端末に顧客情報等の会社機密情報をダウンロードした状態での端末の盗難・紛失は、機密情報の悪用により企業にとって大きな損害を与えることがある。モバイル PC においても SBC では、データが全てサーバで管理されていることから、万一の時にも安心して使用できる。

(c) 通信の暗号化

SBC での C/S システム間の通信はセキュアな鍵交換により接続の各セッションごとに全て暗号化されており、データの盗聴、改ざんを防止できる。

4. SBC でのセキュリティソリューション

(1) サーバベースクライアント

MDIT では、セキュアな SBC 専用端末として以下の 3 種類のサーバベースクライアントを提供している。

- ・TX110 (モニター 一体型)
- ・TX210 (Box 型、モニター別)
- ・TX110-TP (モニター 一体型、タッチパネル付き)



図3. セキュア端末ソリューション TX110, TX210

サーバベースクライアントはディスクを持たず、SBC 対応ソフトのみが動作する SBC 接続専用端末である。ディスク、ファン等の駆動部品を持たないことで高信頼、省スペース、静寂な端末設計であり、こうした専用端末を使用すると可用性を大きく高められるとともに人的なセキュリティを技術的な仕組みとして確保できる。

(a) 情報不正持ち出し防止強化：FDD 等のリムーバブルデバイスを持たないので、不正データ持ち出し防止を更に強化できる。

(b) ウイルス対策：全社員の端末ウイルスソフトを常に最新状態に保つ必要があるが、SBC 専用端末ではディスクを持たないことからウイルス感染の危険が無い(サーバ側の

みウイルスソフトを最新に保つだけで良い)

(c) ブラウザからの不正アクセス対策：ブラウザの脆弱性に対する修正情報が頻繁に発行される中で、各担当者が自己 PC のブラウザを最新状態に保つ必要があるが、SBC では、サーバ側のみ修正情報を適用するだけで良い。

(2) 認証ソリューション

SBC では、常にサーバにログインして動作し、ネットワーク上でのデータは常に暗号化されていることから、ログイン認証を強化することでセキュリティを一層強化できる。MDIT は以下の多彩な認証ソリューションを提供している。



図4. SBC 認証ソリューション (IC カード、指紋)

(a) SBC 専用端末用 IC カード接続認証 EasyLogin

SBC 専用端末上には、サーバへの接続情報を設定することなく、サーバ接続時に IC カードをリーダに挿入し IC カードの暗証番号 (PIN コード) を入力するだけで自動的にサーバ接続できる製品を提供する。物理的な IC カードを持っており、本人しか知り得ない PIN コードによる 2 段階認証によりセキュリティを強化できる。また、端末も IC カード認証が OK とならないと端末自体の操作もできないようになっていることから、セキュリティが高い。IC カードの中にサーバ接続情報とサーバへのログイン情報を持つことにより、公開鍵基盤 PKI (Public Key Infrastructure) のように証明書管理する特別なサーバを必要とせず認証管理も簡単に行える。さらに、Windows が提供する PKI を用いたスマートカードログオンの仕組みも同時に提供する。

(b) PC 用 IC カードソリューション EasyLogin-Web

SBC の端末としては、専用端末だけでなく PC でも利用できる。PC では Web から SBC サーバに接続して SSL (Secure Socket Layer) を利用したセキュアな接続が可能である。これにより、モバイルで出張先から会社の SBC サーバに接続して、オフィスと同じ環境で使用することができる。こうした環境では個人認証が特に重要となる。Web の SBC 接続画面に対して IC カードをセットし、IC カードの PIN コードを入力するだけでサーバ接続可能なソリューションを提供している。

(c) PC 用指紋認証による Web 接続ソリューション

三菱電機(株)稲沢製作所製の指紋付 IC カードリーダライタ装置を用いた指紋認証ソリューションを提供する。PC から Web を利用して SBC サーバに接続する時の個人認証として、指紋を入力するだけで SBC サーバに接続できる。こ

の製品は、ICカードの暗証番号であるPINコードの代わりに、指紋認証により指紋付ICカードの持ち主本人の指紋と照合できて初めてICカードの内部情報を読み出せるようになっており、バイオメトリクスを用いた2段階の個人認証なためICカードよりさらにセキュアな認証ソリューションと言える。さらに、指紋装置だけを用い、サーバ側で指紋照合するソリューションも用意している。

(3) 文書利用権管理システムとSBC連携ソリューション

機密性の高い文書管理において、SBCだけではセキュリティ性を守れない場合も想定される。ある人に文書のアクセス権が付与されている場合(例えばメールの添付文書などの場合)SBC単体では防止しきれないケースでも三菱電機利用権管理ソリューション<DROSY>(注4)を使用し、文書を暗号化することにより、第三者にそのファイルが渡った場合でも不正閲覧を防ぐことができる。また、機密文書の印刷などに対しても利用者の資格に応じた利用制限(例えば印刷不可とする等)を文書ファイルごとに設定可能であり情報漏洩防止が図れる。SBC環境においてサーバベースクライアントのICカードソリューションとDROSYを連携することで、より強固にセキュリティを保持し、利用者へ負担を強いることの無いシステム環境を構築できる。

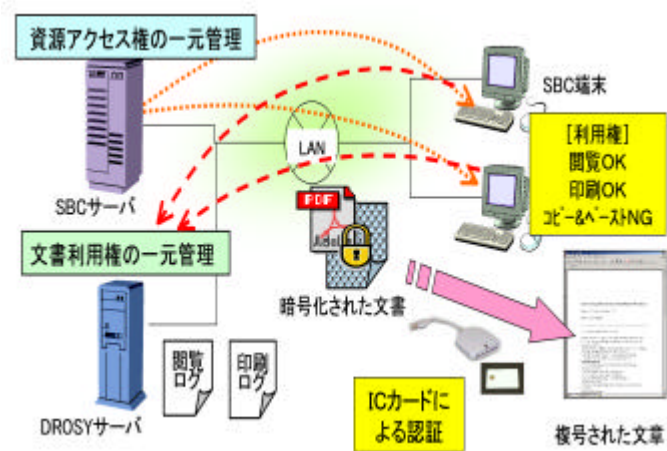


図5 . DROSYにおける文書利用権管理システム

(4) セキュアなSBC設計・構築・保守サービス

SBCはサーバで全てのプログラムが動作し、個人ファイルも含めて全てサーバで管理することから、可用性の高いシステム構築が求められる。サーバのロードバランス設計、アクティブディレクタのセキュリティポリシー設計、ストレージ設計、ネットワーク設計が重要であり、各種SBCシステム設計・構築・保守サービスを取り揃えている。

(5) モバイルSBCソリューション

いつでもどこでも多様な通信手段を用いてSBCサーバに接続することで、社内でも外出先でも自宅でもオフィスと同じ環境を安心して利用できるモバイルSBCソリューション

を提供している。

5 . 事例

(1) 経理業務アウトソーシング会社納めSBC構築事例

経理業務のアウトソーシングを受ける会社であるため、お客様の個人情報を大量に扱っていることから、お客様からも理解できる形でのセキュリティ強化が必要であった。そこで、SBCとサーバベースクライアントを導入し、お客様の個人情報漏洩防止のためにセキュリティを強化した。

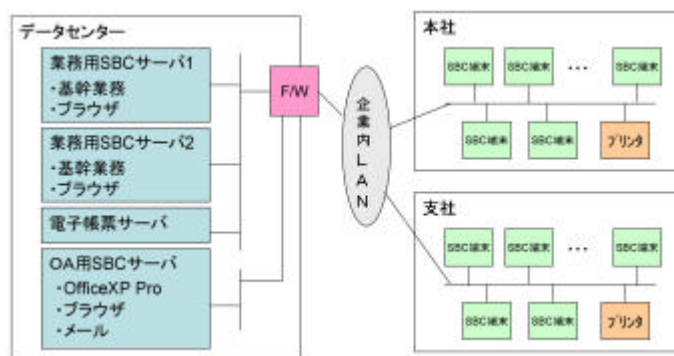


図6 . 経理業務アウトソーシング会社納めSBC構築事例

(2) SBCによるWeb対応インターネット接続事例

SBCのWeb接続機能を利用し、既存のC/SシステムをそのままWebブラウザから接続可能とし、ICカードソリューションEasyLogin-Webを利用して個人認証することで、各支店・支社から、本社のSBCサーバにインターネット接続でのセキュアなアクセスを可能にした。

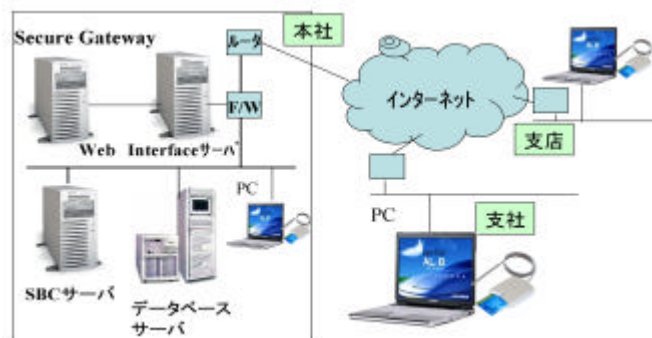


図7 . SBCによるWeb対応インターネット接続事例

6 . おわりに

運用/人的なセキュリティ面を技術的な仕組みとして向上させ、いつでもどこでも接続すればそこがオフィスとなるSBCセキュリティソリューションを紹介した。

SBCは、単にセキュリティ強化だけでなく、運用管理コスト削減においても非常に効果のあるソリューションであり、サーバ、端末、ソフトウェア、構築を含むトータルなSBCソリューションに更なる改善をしていく所存である。

(注4) 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。