巻頭論文

クラウド技術を適用した企業情報システムへの取組み


伏見信也* 茂木 強**

Cloud Computing Technologies for Enterprise Information Systems

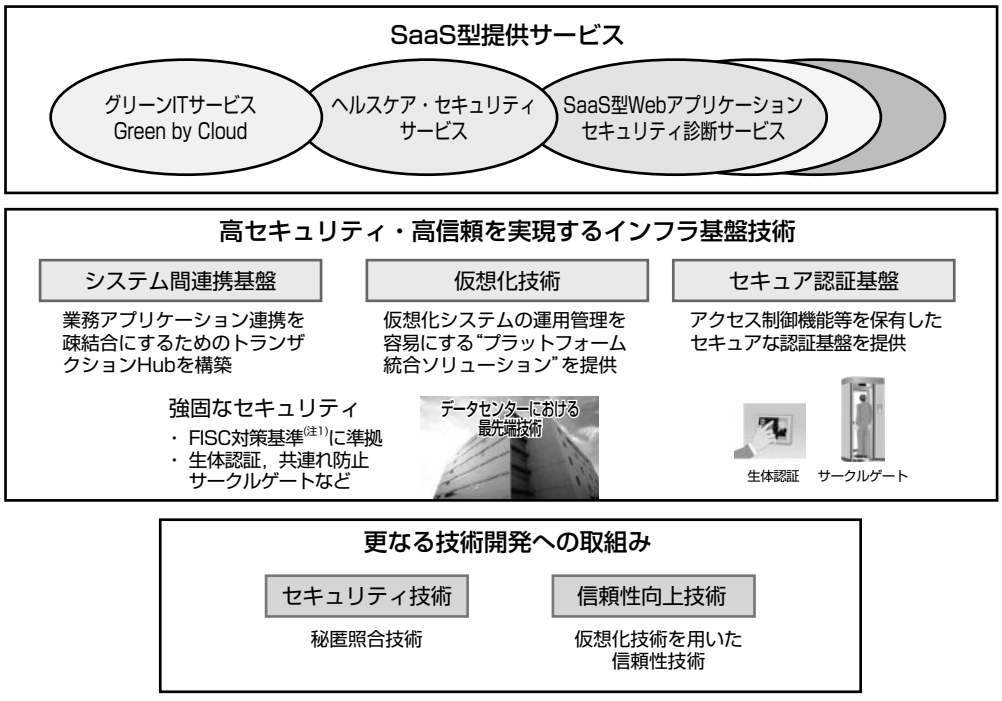
Shinya Fushimi, Tsuyoshi Motegi

要 旨

ITインフラやアプリケーションをサービスとしてユーザーに提供するというクラウドコンピューティング(以下“クラウド”という。)の流れが加速している。しかし，インターネットにアクセスできればだれでも利用可能なオープンなクラウド(パブリッククラウド)では，ユーザーが信頼性やセキュリティなどに不安を感じることもあり，企業情報システムでの利用が進展していない。そのため，企業情報システムにおけるクラウド利用に関しては，特定の限られたユーザー(企業内，企業グループなど)に閉じた形で導入し，ユーザーニーズに応じた高いサービスレベルを保証することが必要である。

三菱電機では，高セキュリティ・高信頼性を実現するインフラ基盤技術を保有しており，それを付加価値として，クラウド技術を適用した企業情報システムへの取組みを推進している。その具体的な例として，企業環境の変化に柔軟に対応するためのシステム間連携基盤，容易な運用管理を特長とする仮想化技術，セキュアな認証基盤とアクセス制御技術などのインフラ基盤技術を活用し，セキュリティや省エネルギーを付加価値としたSaaS(Software as a Service) 型サービスを実現している。また，三菱電機情報ネットワーク㈱(MIND)の豊富な実績に基づき，強固なセキュリティを確保したデータセンターによる運用管理サービスなどを提供している。

今後の更なる技術開発の取組みとしては，①復号情報の漏えいの心配を払拭(ふっしょく)するため，暗号化したまま個人識別情報を照合する秘匿照合技術，②仮想化技術を用いた情報システムの信頼性向上技術などの研究開発を行っており，安全性と信頼性を確保した付加価値の高い企業向けITサービスの提供を推進していく。



(注1) (財)金融情報システムセンター：金融機関等コンピュータセンター安全対策基準

クラウド技術を適用した企業情報システムへの取組み

当社では，高セキュリティ・高信頼性を実現するインフラ基盤技術を保有し，それを付加価値として，クラウド技術を適用した企業情報システムを提供する。また，当社の基盤技術を活用した製品と連携し，セキュリティ・省エネルギーを付加価値としたSaaS型サービスを実現している。さらに数年先を見据え，将来的な技術の研究開発を行っており，安全性と信頼性を確保した企業向けITサービスの提供を推進していく。

*インフォメーションシステム事業推進本部 技術企画部長(工博) **情報技術総合研究所 情報技術部門統括

1. まえがき

ITインフラやアプリケーションをサービスとしてユーザーに提供するというクラウドコンピューティング(以下“クラウド”という。)の流れが加速している。ITリソース調達の柔軟性や費用対効果の面から，企業情報システムのプラットフォームとしても魅力的である。しかし，不特定多数のユーザーがインターネット経由で利用できるパブリッククラウドは，信頼性やセキュリティなどのサービスレベルが明確に規定されていないことが多く，企業システムとしての利用を躊躇(ちゅうちょ)させる一因となっている。

当社では，高セキュリティ・高信頼性を実現するインフラ基盤技術をベースに，特定の限られたユーザー(企業内，企業グループなど)に閉じた形での利用を前提として，クラウド技術を適用した企業情報システムへの取組みを推進している。

本稿では，具体的なサービス内容とそれらを実現するための基盤技術，及び将来に向けた最新技術の研究内容について述べる。

2. クラウドの現状

2.1 クラウドとは

図1に示すように，従来の情報システムでは“ユーザーがハードウェアやアプリケーションを自前で購入・管理”していたものから，クラウドでは“情報システムをユーザー側で所有せず，サービスとして使用した分を支払う利用形態”となる。例えば，従来はパッケージソフトウェアを購入して利用していた形態から，クラウドではネットワーク経由でアクセスしてアプリケーションを利用する形態に変わる。

また，クラウドで利用できるサービスは，XaaS(X as a Service)という言い方で大きく3つに分類される(**表1**)。

2.2 クラウドへの期待と懸念

ユーザーから見たクラウドへの期待と懸念については，いろいろなメディアを通じて報告されている。一般に言われているところでは，期待としては，①ITリソースを柔軟に拡張，縮小できること，②サービス開始までの期間が短くて済むこと，③自前でシステムを構築しないので初期投資が抑制されコスト削減が図れること，というような点が挙げられている。

次に利用に際しての懸念事項を**図2**に示す。

図2から，①重要な情報を外部の事業者に預けるというセキュリティ上のリスク，②従来に比べて本当にコストダウンできるか，③サービスレベルが不明瞭(ふめいりょう)，又はサービスレベルが保証されていないというリスク，④社内システムとの連携の困難さなどがクラウドを利用する際の懸念材料になっていることがわかる。

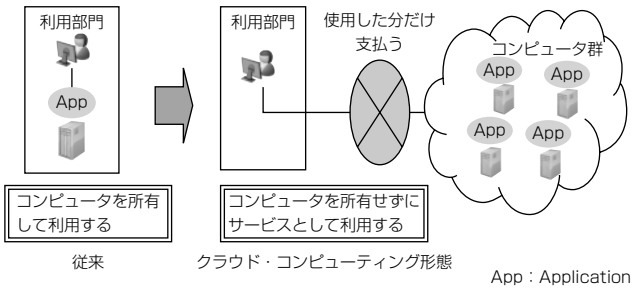


図1．クラウドコンピューティングの概念

3. 三菱電機グループの取組み

2. 2節で述べたような，クラウドの利用におけるユーザーの懸念を解消するために，次のような方策を実現することが必要となる。

(1) 個人情報などの重要なデータを安心・安全に保管できる強固なセキュリティ機能を持つデータセンターと，その運用管理基盤を提供できること

(2) 情報漏えい対策などのために，セキュアな認証基盤を提供できること(特定のユーザーだけがアクセス可能であることを保証するアクセス制御機能など)

(3) 社内の業務システムとの連携を容易に行うことができるシステム間連携手段を提供できること

(4) (1)～(3)で述べた基盤を活用し，サービスレベルを保証したSaaS型サービスとその基盤を提供できること。

三菱電機グループではこれらの実現に当たり，セキュリティ及び信頼性を担保するため，不特定多数のユーザーが利用するパブリッククラウドではなく，特定の限られたユーザー(企業内，企業グループ向けなど)によって独占的又は排他的に利用できる“プライベートクラウド／マネージドクラウド”を対象に，そのシステム構築や運用管理サービス，SaaS型サービスの提供を推進している(**図3**)。

表1．クラウドのサービス分類

サービス分類	内容
SaaS(Software as a Service)	アプリケーションを提供するサービス
Paas(Platform as a Service)	アプリケーションの開発環境，実行環境を提供するサービス
IaaS(Infrastructure as a Service)	ITリソース(仮想マシン，OS，ストレージ等)を提供するサービス

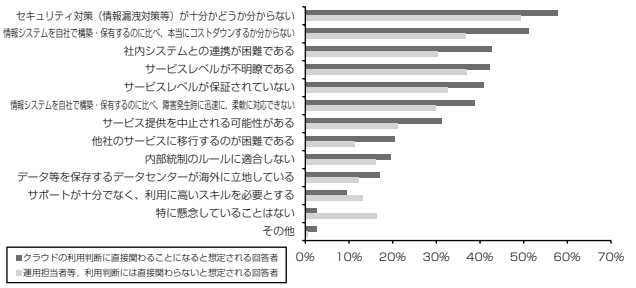


図2．クラウドコンピューティングの利用を控える理由／利用に当たっての懸念(1)

なお本稿では，自社内のデータセンターに情報システムを設置する形態を“プライベートクラウド”，社外のデータセンターに委託する形態を“マネージドクラウド”と呼ぶ。

三菱電機グループの具体的な取組み内容を**表2**に示す。太陽光発電システムを採用したMINDの最先端データセンター，仮想化やセキュア認証などの基盤技術，これらの技術に基づく各種SaaSサービスについて，次に代表的な事例を述べる。詳しい内容に関しては，この特集号の該当する論文を参照されたい。

3.1 高セキュリティ・高信頼を実現するインフラ基盤技術

3.1.1 データセンターにおける最先端技術

MINDの最新データセンターでは，重要なシステムを震災から保護するためにビル全体を免震構造とするとともに，集積度の高いシステムを収容するための高度な冷却技術を採用するなど，堅牢(けんろう)なファシリティを実現している。また，サーバ室へのアクセスに生体認証と共連れ防止のサークルゲートを組み合わせることで厳密な入退室管理を行い，高度な物理セキュリティを確保した。

ネットワークについては，マルチキャリアによる多様かつ高速な接続を準備するとともに，負荷分散・帯域制御等のトラフィック制御技術によってトラフィック増に対応する。これらに加え，各種の省電力設備の採用と太陽光発電システムの導入によって，地球環境に配慮しながらクラウド技術への適応を実現している。

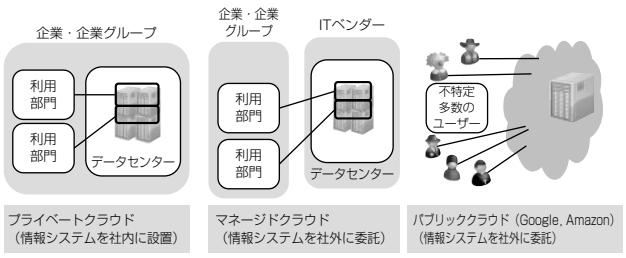


図3．当社の取組み形態

表2．三菱電機グループの取組み内容

分類	社名	取組み内容
高セキュリティ・高信頼を実現するインフラ基盤技術	MIND	データセンターにおける最先端技術
	MDIT	仮想化技術(VMINTEGRA)
	MDIS，MIND ジャパンネット㈱	セキュアな認証基盤技術
	MDIT	システム間データ連携基盤技術
SaaS型提供サービス	MDIS MDIT	グリーンITサービス (Green by Cloud)
	MDIS ジャパンネット㈱	ヘルスケアセキュリティサービス
	MIND	SaaS型セキュリティ診断サービス
将来技術	三菱電機㈱ (情報技術総合研究所)	秘匿照合技術 仮想化技術を用いた信頼性向上技術

MDIS：三菱電機インフォメーションシステムズ㈱
MDIT：三菱電機インフォメーションテクノロジー㈱
MIND：三菱電機情報ネットワーク㈱

3.1.2 仮想化技術

サーバ仮想化技術が急速に進歩しており，この数年で大企業を中心に仮想化によるサーバ統合が進展してきた。しかしまだ，サーバ統合におけるリソース設計，パフォーマンス評価，仮想環境構築ノウハウを持つ技術者は不足しており，そのために構築・運用コストは高く，仮想化による中小規模サーバ統合普及の阻害要因となっている。

三菱電機インフォメーションテクノロジー㈱(MDIT)は，これらの課題を解決するため，プラットフォーム統合ソリューション“VMINTEGRA(ヴイエムインテグラ)”を開発・製品化した。VMINTEGRAは，仮想化市場で高いシェアと実績のあるVMware社のVMware(注2) vSphere4に運用監視機能をパッケージした製品で，“簡単導入”“簡単運用”“安心サポート”の3つのコンセプトの下，中堅・中小企業でのサーバ統合の促進を目指している。

3.1.3 セキュアな認証基盤技術

企業や医療機関などに各種のサービスを提供する場合，アプリケーションやネットワーク等の様々なレベルで，利用者に応じたアクセス制御が重要であり，セキュアな認証基盤を確立する必要がある。

認証情報は個人情報であり，高度な機密情報であることから，それらは企業内のシステムに安全に保管した上で，外部のクラウドシステムと既存の企業内システム間での認証連携を実現する方式を確立した。認証機能やデータのアクセス制御機能の実装に当たり，SAML(Security Assertion Markup Language)やXACML(eXtensible Access Control Markup Language)といった標準仕様を採用し，オープンソースソフトウェアも活用しながら，再認証が不要なシングルサインオン機能を独自に開発し，実証実験を通してその有効性を確認した。

3.1.4 システム間データ連携基盤の構築

トランザクションHubとは，トランザクションデータを蓄積して，そのデータを再利用する業務アプリケーションとの間で交換する“データ交換の場”である。一般に，業務アプリケーションを単純にSaaS化すると，社内のシステムとSaaS化したシステムの間の連携が分断されてしまうという問題点がある。

業務アプリケーションはトランザクションHubを経由してデータを交換することで，他の業務アプリケーションの影響を受けない独立した部品となる。そのため，システムの交換，新たなシステムの追加，SaaS化等を容易に実現することが可能となる。

3.2 SaaS型提供サービス

3.2.1 グリーンITサービス“Green by Cloud”

2010年4月から施行された改正省エネ法では，“事業者単位”でのエネルギー管理が義務付けられるようになった

(注2) VMwareは，VMware, Inc. の登録商標である。

ため，ビルのオーナーだけでなく，そこに入居しているテナント事業者もエネルギー使用量を把握する必要がある。そこで当社では，ビルオーナーとテナントが協力して環境情報データの見える化等に取り組み，課題を解決するグリーンITサービス“Green by Cloud”の提供を開始した。これは，三菱電機グループの総合力を生かし，ビルや工場内の設備・機器，セキュリティシステムとITシステムをネットワークで接続し，建物を丸ごと省エネルギーする新しいサービスである。

Green by Cloudは，CO_2排出削減施策のPDCA（計画・実行・評価・改善）サイクルを支援するトータル環境経営ソリューション“DIALCS”，大量に発生する環境情報データを分析する環境経営ソリューション“MELGREEN”，及びこれらが動作する最先端のデータセンターをサービス基盤としている（**図4**）。このサービスによって，法規制の対応に加え，ビルオーナーはビルの付加価値向上，テナントは企業価値の向上というメリットが得られる。

3.2.2　ヘルスケアセキュリティSaaSへの取組み

ヘルスケア分野では，医療情報等の機微な情報を取り扱うため，情報システムの管理・運用でも特段の配慮が求められる。三菱電機グループでは，厚生労働省等のガイドラインを遵守できる低コストのハイレベルセキュリティサービスを医療機関等に提供することを目指して，ヘルスケアセキュリティSaaSシステムの構築と評価を実施した。

これらの成果をベースに，円滑な医療情報交換や保存が義務付けられた医療情報の外部保存を行える環境の提供を実現していく。また，真正性を担保するための電子署名・タイムスタンプ付与をSaaS型サービスとして提供し，電子署名付き文書の文書交換や外部保存に対応したサービスと連携し，ワンストップで地域医療連携のニーズにこたえていく（**図5**）。

4. 更なる技術開発への取組み

従来以上の高セキュリティ・高信頼を実現するための研究開発として，暗号化したまま個人識別情報を照合する技術と仮想化技術を用いた信頼性向上技術について述べる。

4.1　クラウド時代の個人認証“秘匿照合技術”

近年，ネットワーク経由でサービスを利用するクラウドの進展によって，電子メール運用や文書管理をデータセンターに委託する需要が高まっている。この際に使われる本人認証は，事前に登録した個人識別情報と認証時に入力される個人識別情報を照合して行われるが，個人識別情報は厳格な保護が求められることから，暗号化した上でデータセンターに送られ管理される。しかし，これまで提案されている技術では，照合する際に復号が必要なケースや，暗号化情報からその一部が類推可能なケースがあるなど，復号情報の漏えいの可能性を完全には否定できないという問題があった。また，登録者数が多くなると認証に時間がかかるという問題を持つものもある。

三菱電機は，復号することなく暗号化したまま個人識別情報を照合する秘匿照合技術を開発した（**図6**）。これによって，データセンター内の個人識別情報の利用・管理を安全に効率良く行えるようになる。顔・指紋・筆跡・文字・

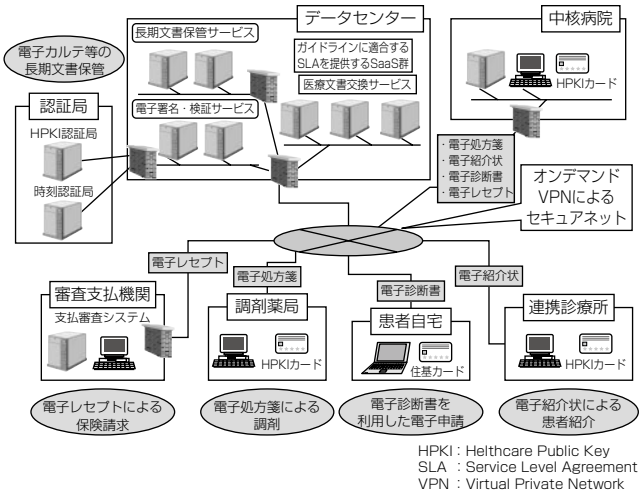


図5．ヘルスケアセキュリティSaaSの概念図

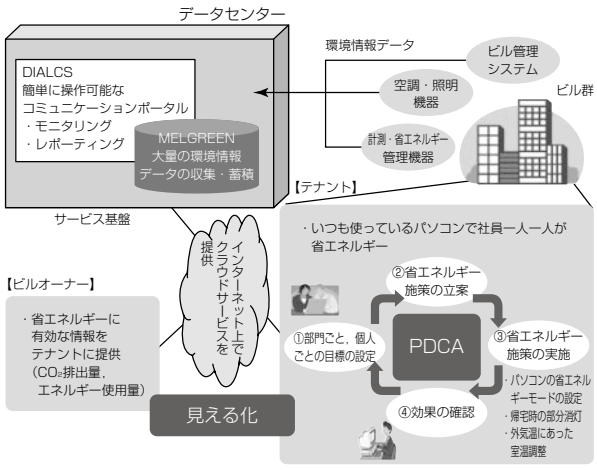


図4．Green by Cloudとサービス基盤

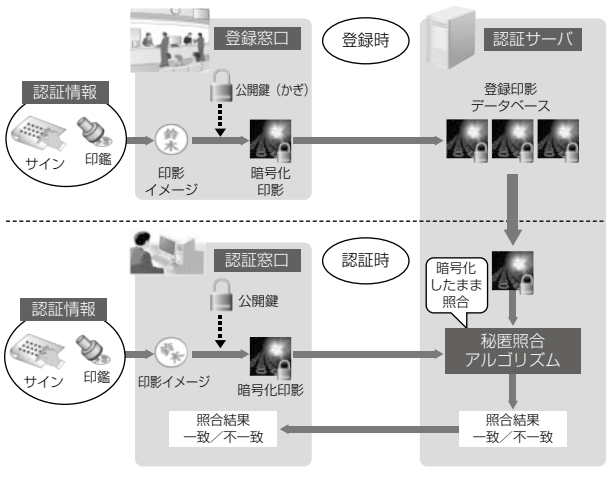


図6．秘匿照合技術

印影などの個人識別情報は，一般的に複数の特徴で表現される。例えば，顔は，輪郭，色，大きさ，目と鼻の位置関係など，複数の特徴を数値化し，その数字の組（特徴ベクトル）で表現される。本人認証は，認証時に取得した特徴ベクトルを登録時の特徴ベクトルと比較し，両ベクトルの距離から類似，又は一致した場合に同一人物と判定する。したがって，この特徴ベクトルは厳格な管理が必要であり，特徴ベクトルは暗号化され認証サーバに格納される。

この秘匿照合技術は，2つの暗号情報の算術演算が可能な準同型暗号を用い，暗号化された特徴ベクトル間の距離を，認証サーバとの1度のやり取りで照合する。これによって，照合の過程で特徴ベクトルが復号されることなく，データセンターにおける個人情報の秘匿が，少ない通信時間で実現できる。

4.2　仮想化技術を用いた情報システムの信頼性向上技術

重要な社会インフラを支える情報システムでは，サーバを2重系構成として信頼性を高めている。2重系サーバでは，稼働中のメインサーバが故障した際，待機サーバに切り替えて業務を継続できるが，故障したサーバが復旧するまでの間は信頼性が低下するので2重系へのすみやかな復旧が求められる。2重系以上の信頼性を持たせるには，業務ごとに予備専用のサーバを準備する3重系構成が必要であり，また，データの保存に，信頼性の高い高価な外部共有ディスクを用いる構成が採用されており，情報システム構築コストの増大に結びついている。三菱電機は，仮想化技術によって，システムを構成するサーバ群の空き資源を活用して，2重系構成を短時間で復旧する技術を開発した（**図7**）。この技術によって，3重系構成と同等の信頼性を確保しながら，予備専用サーバと外部共有ディスクを不要とし，システムの構築コストを抑制できる。

サーバの仮想化技術によって，サーバ群の空き資源（CPU（Central Processing Unit），メモリ，ディスクなど）を活用して故障したサーバと同等の処理ができる代替環境を自動で構築し，2重系構成に復旧する。これによって，3重系構成と同等の信頼性を確保しながら，予備専用サーバ群は不要となる。

また，各仮想サーバの実行環境であるOSやアプリケーションのみならず，代替環境の構築に必要な復旧用データもすべて，情報システムを構成するサーバ群の内蔵ディスクに格納する。復旧用データは，各仮想サーバで共通のOS部分と，固有のアプリケーション部分に分けて格納することで必要なディスク容量を削減しており，これによって，高価な外部共有ディスクを使用する必要がなく，システムを低コストで構築でき，万が一共有ディスクが故障した際の全業務停止のリスクも回避可能となる。

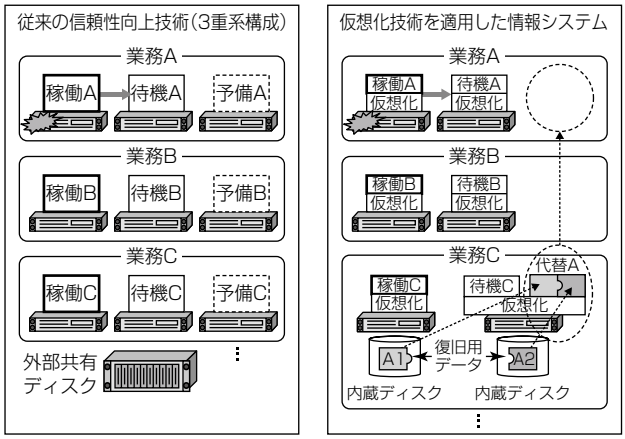


図7．仮想化技術を用いた信頼性向上技術

5. むすび

企業情報システムへのクラウド技術の適用に対する期待が高まっている一方，セキュリティや信頼性の面で不安を感じるユーザーも多く，これらの不安感を払拭するための努力が必要である。

三菱電機では，これまで培ってきた高信頼・高セキュリティのインフラ基盤技術に関する豊富な経験を生かすとともに，数年先を見据えた独創的な研究開発も並行して進めており，今後も付加価値の高い企業向けITサービスの提供を推進していく。

参考文献

(1)　経済産業省：情報システム・ソフトウェアの信頼性及びセキュリティの取組強化に向けて～豊かで安全・安心な高度情報化社会に向けて～―中間報告書―（2009）