TREND

個人情報保護法と東芝の情報セキュリティ技術

Personal Information Protection Law and Toshiba Information Security Technologies

由良　浩司　　新保　　淳

■YURA Koji　　■SHIMBO Atsushi

個人情報漏えいの事故が後を絶たないなか，「個人情報の保護に関する法律」（以下，個人情報保護法と略記）が2005年4月に全面施行された。この法律は個人情報取扱事業者の義務を定めており，この中で「個人データの安全管理のために必要かつ十分な措置」を講じるよう求めている。情報システムは，その高い能力を最大限に引き出そうとするために，従来ややもすると利便性が優先され，セキュリティが維持されずに結果として様々な問題を生じてきた。個人情報保護法への対応を通じて情報セキュリティへの意識が高まり，社会に不可欠な基盤である情報システムがより安全性の高いものとなることが期待される。

東芝グループは，安心・安全な社会を築く基盤となる技術として，情報セキュリティ技術の研究開発に全力を挙げて取り組んでいる。

The Personal Information Protection Law has been fully in force since April 2005 in Japan, against the background of personal data divulgence cases being reported in the newspapers almost daily. Under the law, holders of personal data must now take sufficient measures to maintain their data safely. The convenience of information systems often takes precedence over information security, and insecure information systems have caused many problems. There is now a greater interest in information security because of the law, and the development of more secure information systems as infrastructure is desired.

The companies of the Toshiba Group are making maximum efforts to develop products and services based on information security technologies, forming the foundations of a safe and secure society.

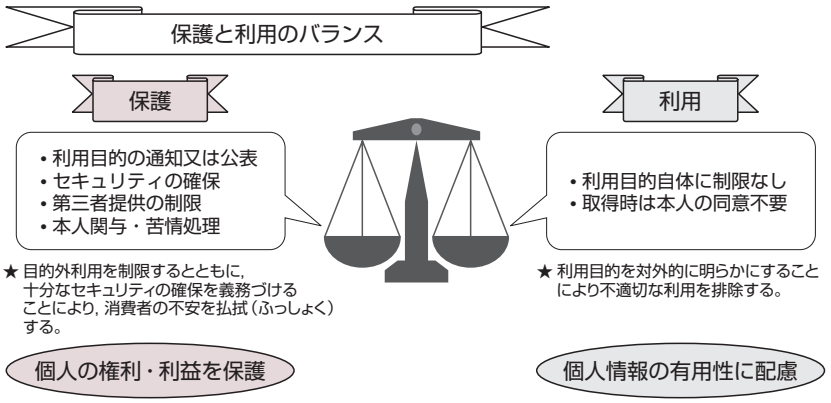
個人情報保護法

個人情報の漏えい事件・事故

高度情報通信社会の進展により，個人情報の利用が急速に拡大している。その一方で，情報システムで管理運用されている個人情報の漏えい事件・事故が後を絶たない。2004年2月には，インターネット接続サービス会社から460万人分の顧客情報が漏えいしたと報じられた。その後も漏えい事件・事故は続き，2005年に入っても毎日のように報じられてきた。

個人情報保護法

このような状況の下で，2005年4月に個人情報保護法[(1)]が全面施行された。この法律は「個人情報の有用性に配慮しつつ，個人の権利・利益を保護すること」を目的とする，個人情報の適切な取扱いに関する法律である（**図1**）[(2)]。



出典：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（概要）[(2)]

図1．個人情報保護法の考え方 ― 法律の目的は個人情報の有用性に配慮しつつ，個人の権利と利益を保護することである。

Concept of Personal Information Protection Law

この法律の第4章第1節（第15条から36条）では，個人情報を取り扱う事業者の遵守すべき義務について規定している。第20条では「個人情報取扱事業者は，その取り扱う個人データの漏えい，滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と定めている（安全管理措置）。

経済産業省ガイドライン

個人情報を取り扱う事業者の遵守すべき義務については各省庁がガイドラインを定めている。なかでも経済産業省のガイドライン[(3)]は多くの事例を掲載して具体的に書かれており，各所から参照されている。経済産業省ガイドラインでは，安全管理措置について4分野18項目を挙げて事業者に求められる対応を詳細に定めている(**囲み記事参照**)。

東芝グループの対応

東芝グループ企業の多くも，やはり個人情報取扱事業者であり，その対応を行っている。2004年10月には東芝社内に“情報・セキュリティセンター”を設立

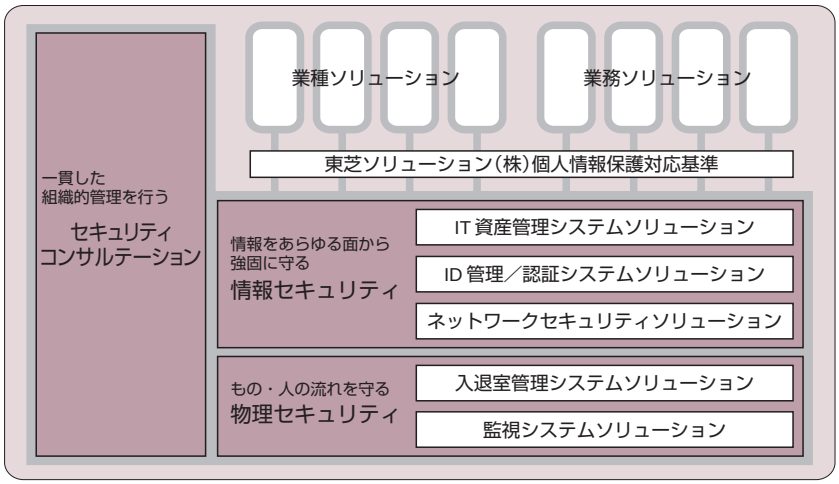


図2．東芝ソリューション(株)が発表した個人情報保護対応ソリューションの構成 ― 情報セキュリティ，物理セキュリティ，コンサルテーションから構成される基盤ソリューションと，基盤ソリューションをベースとして対応基準に沿って開発される業種，業務ソリューションから成る。

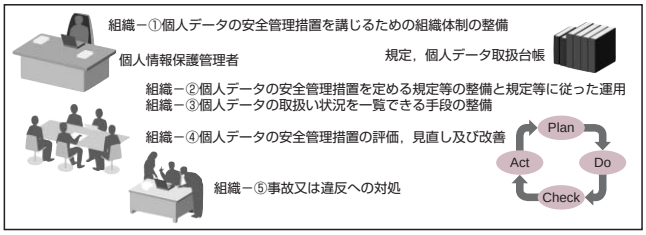
Personal data protection-ready products and services

経済産業省ガイドラインの定める安全管理措置

経済産業省ガイドラインの定める安全管理措置では，個人情報保護法第20条関連の安全管理措置について，4分野18項目にわたり説明している。18項目すべてに対して，「講じることが望まれる事項」として合計59項目の対策が具体的に記述されており，個人情報を扱う情報システムを構築するうえで，規範となる文書となっている。

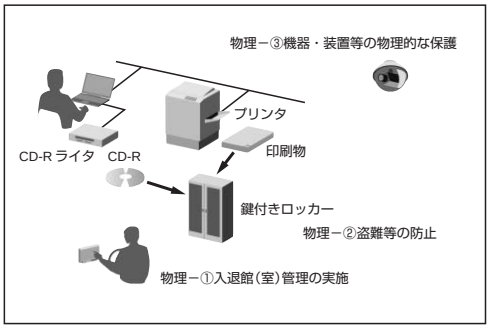
組織的安全管理措置

① 個人データの安全管理措置を講じるための組織体制の整備
② 個人データの安全管理措置を定める規定等の整備と規定等に従った運用
③ 個人データの取扱い状況を一覧できる手段の整備
④ 個人データの安全管理措置の評価，見直し及び改善
⑤ 事故又は違反への対応



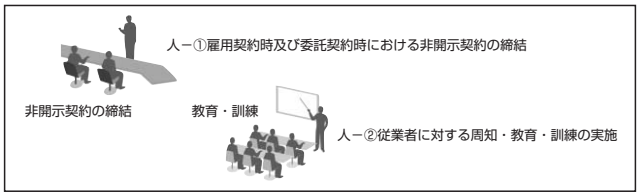
物理的安全管理措置

① 入退館(室)管理の実施
② 盗難等の防止
③ 機器・装置等の物理的な保護



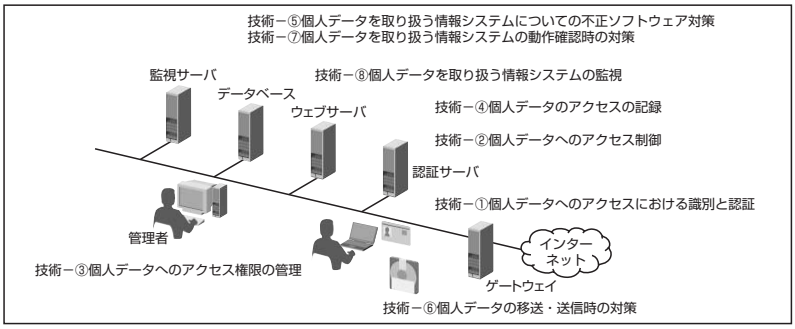
人的安全管理措置

① 雇用契約時及び委託契約時における非開示契約の締結
② 従業者に対する周知・教育・訓練の実施



技術的安全管理措置

① 個人データへのアクセスにおける識別と認証
② 個人データへのアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データのアクセスの記録
⑤ 個人データを取り扱う情報システムについての不正ソフトウェア対策
⑥ 個人データの移送・送信時の対策
⑦ 個人データを取り扱う情報システムの動作確認時の対策
⑧ 個人データを取り扱う情報システムの監視



出典：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[(3)]

し，密接な連携を必要とする情報セキュリティと個人情報保護の体制を一元化することにより，施策実行の一貫性強化とスピードアップを図っている[4]。

また，東芝ソリューション(株)では，独自の“個人情報保護対応基準”を作成し，様々な業種・業務に向けたシステムソリューションのセキュリティ機能を強化して，この基準に適合させていこうとしている[5]。経済産業省ガイドラインに定められている安全管理措置の4分野のうち，「組織的安全管理措置」と「人的安全管理措置」をセキュリティコンサルテーションにより，「物理的安全管理措置」を物理セキュリティにより提供し，「技術的安全管理措置」は情報セキュリティを基盤として実現していく(**図2**)。

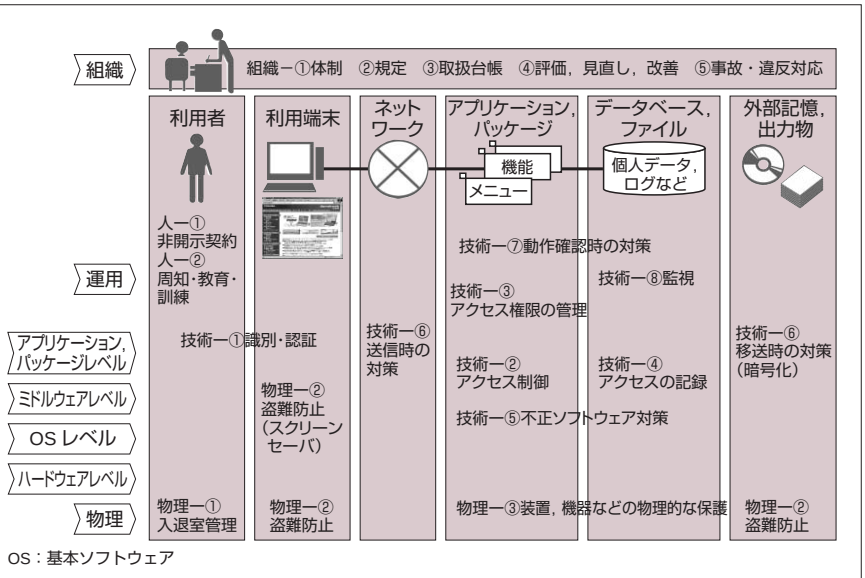


図3．安全管理措置18項目の情報システムへのマッピング ― 安全管理措置が情報システムとその環境全般に及んで講じられる必要がある。なお，分野と項目番号(①～⑧)は囲み記事に対応している。

Eighteen measures for personal data security defined by Ministry of Economy, Trade and Industry

東芝の情報セキュリティ技術

情報システムと東芝の情報セキュリティ技術

図3は，経済産業省が定める安全管理措置の18項目を，情報システムとその環境に位置づけたものである。安全管理措置が，情報システムとその環境全般に及んで講じられる必要があることが見てとれる。

この特集では，個人情報保護法対応を中心として，企業組織の情報セキュリティを確保する東芝ソリューション(株)の取組みと，東芝 研究開発センターで開発されているセキュリティ基盤技術を取り上げている。**図4**は，この特集で紹介している情報セキュリティ技術の位置づけを図3にオーバラップさせたものである。情報システム全体にわたり，安全管理措置18項目の多くをカバーしていることが見てとれる。以下ではこれら各技術の概要を紹介する。

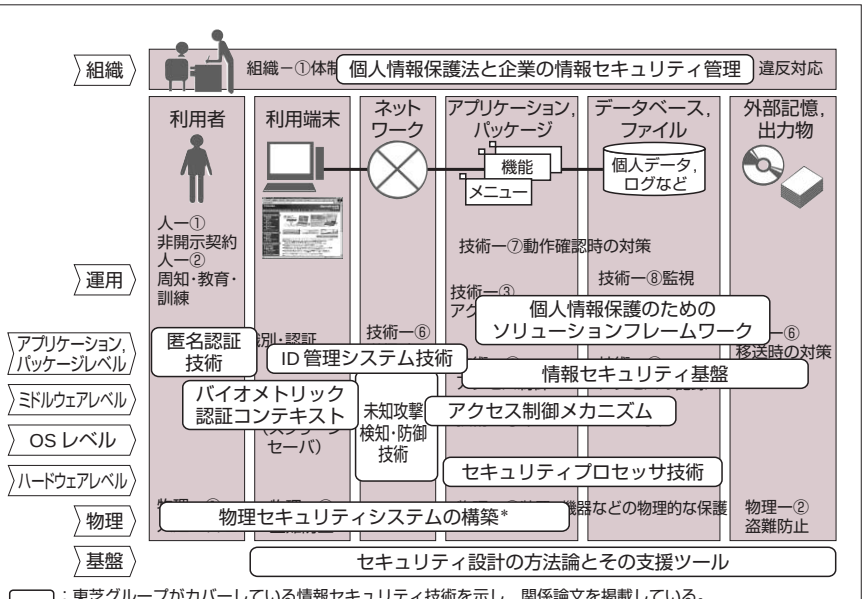


図4．東芝グループ情報セキュリティ技術の情報システムへのマッピング ― 東芝グループ情報セキュリティ技術は情報システム全体にわたり，安全管理措置4分野の多くをカバーしている。

Mapping of Toshiba information security technologies on information system architectures

セキュリティソリューション

東芝ソリューション(株)は個人情報保護法の全面施行を受けて，法律が求める安全管理措置などのセキュリティ確保に企業や組織と共に取り組んでいる。“個人情報保護法と企業のセキュリティ管理”(p.7－10)では，個人情報保護法が求める安全管理措置など，企業や組織に求められているセキュリティ確保を確実に実施するために，情報セキュリティマネジメントシステム(ISMS)を活用する方法とそのコンサルテーションについて紹介する。

東芝ソリューション(株)が提供する情報システムの中には，顧客が業務において個人情報データベースを扱うためのシステムも多い。そこで，“個人情報保護対応基準”を作成するとともに，業種・業務システムとセキュリティ基盤シ

ステムとを連携させる，“個人情報保護のためのソリューション フレームワーク”（p.11－14）を確立した。システムソリューションにこの基準を適用することによりセキュリティ機能を強化・向上し，また，システムを運用する顧客が個人情報保護法への対応状況を的確に把握することを可能にするフレームワークである。

“情報セキュリティ基盤の考え方と東芝のソリューション”（p.15－18）では，業種・業務ソリューションと連携する情報セキュリティ基盤について紹介する。東芝ソリューション（株）が提供する情報セキュリティ基盤では，上流のコンサルティングにより企業・組織ごとに持つ課題を洗い出し，更に，その企業が持つ組織風土などを踏まえて，定着するセキュリティをいかに構築するかを考え，そのうえで必要なセキュリティシステムを提案している。

識別・認証技術

情報システムでの不正行為の多くはその背景として，システムがユーザーを正確に識別していないことを悪用されており，例えば，情報漏えいの大部分は組織内関係者により行われている。情報システムの識別・認証を中心とする技術的安全管理措置を十分にとっていれば，漏えい事件を大幅に減らすことができる。しかし，情報システムの識別・認証を単純に強化するだけではユーザーにとって負担となるうえに，システム管理コストも増大する。“管理コスト削減とシステム向上を実現するID管理システム技術”（p.19－22）では，管理コストの削減，セキュリティの向上，ユーザー負担の軽減を同時に実現できるID（IDentification）管理システムを紹介する。

個人情報保護法の完全施行により個人情報の管理コストが大きくなり，インターネットショッピングサイトでは，決済や商品の発送を行うための個人情報をやむをえず取得している場合も多い。このようなショッピングサイトに適しているのが“匿名認証技術とその応用”（p.23－27）である。匿名認証を使えば，店舗は不必要に顧客情報を保持する必要がなく，顧客は自分の名まえなどを明かさずに気楽にショッピングができる。

“バイオメトリック認証コンテキスト”（p.28－31）は，バイオメトリック本人確認プロセスを実行するICカードやバイオメトリックデバイスなどのエンティティが，各自の実行した本人確認プロセスに関する情報及びその結果を保証して検証者へ通知するためのフォーマットである。バイオメトリック認証コンテキスト（BAC）により，インターネットなどのリモート環境におけるバイオメトリック認証が可能になるとともに，バイオメトリクスのウェブサービスへの応用が期待される。

ネットワークのセキュリティ

セキュリティホールの存在が知られてからそれを利用した攻撃が現れるまでの時間が非常に短くなり，従来の不正侵入防御装置では対処しきれなくなっている。そこで，ネットワークのアプリケーション層で常に学習しながら統計分析するL7パラメトリック分析方式™による未知攻撃検知・防御技術を開発し，タグチメソッドを用いて高い検知精度を実現した（“ネットワークに対する未知攻撃の検知・防御技術とその応用”（p.32－35））。

セキュリティ基盤技術

情報セキュリティの基盤技術として，暗号技術や電子透かし技術の重要性に変わりはない。一方で，特に暗号技術は実際に多くのシステムで活用されるレベルにまで成熟してきたことも事実である。そこで，この特集では，これら基盤技術を利用して構成されるセキュリティ システムやネットワークセキュリティにおける要素技術の研究成果を紹介している。

“サーバ アプリケーションを保護するアクセス制御メカニズム”（p.36－39）は，リモート アクセス環境における，サーバ アプリケーションの実装上のぜい弱性を利用した攻撃やDoS（Denial of Service）攻撃などを防止する要素技術である。TCP（Transmission Control Protocol）におけるSYNパケットに認証用情報を埋め込み，認証に成功した場合にだけTCPコネクションの確立を行う手法を考案した。

“セキュリティ構築方法論とその支援ツール”（p.40－43）は，安全な情報システムを構築するために，システムのセキュリティ分析やセキュリティ機能の設計を行ううえでの方法論と支援ツールを試作したものである。ここでの設計情報は，ISO/IEC（国際標準化機構／国際電気標準会議）15408（Common Criteria）に基づいたセキュリティ評価手順における設計文書の作成にも利用できる。

“オープンソースOSと共存可能なセキュリティプロセッサ技術”（p.44－47）は，仕様が公開されたオープンな計算機環境における，セキュリティを考慮したプロセッサアーキテクチャの提案である。ここで対象とした脅威は，計算機上で動作するソフトウェアのリバースエンジニアリングやコンテンツの不正コピーなどである。

いずれの内容もプロトタイプの試作や支援ツールの開発を行い，実際に有効性を検証している。

情報セキュリティ確保の取組み

情報システムは，その高い能力を最大限に引き出そうとするために，従来ややもすると利便性が優先されセキュリティが維持されずに，結果として様々な問題を生じてきた。ISO/IEC17799では，情報セキュリティを「情報の機密性，完全性，及び可用性の維持」と定義している。この定義によれば，現在の情報システムは，可用性を優先するあまり機密性と完全性が維持できていないものが多く，相次ぐ個人情報の漏えい事件・事故はその現れであると理解できる。

個人情報保護法への対応を通じて情報セキュリティへの意識が高まり，社会

に不可欠な基盤である情報システムがより安全性の高いものとなることが期待される。企業には，顧客情報以外にも，マーケット情報，販売計画，商品企画，設計情報など重要な秘密情報が多く存在し，そのほとんどが情報システムで管理されている。これらの情報の漏えい事件・事故は企業の存亡にかかわる重大なリスクであり，これらの情報を扱うシステムも個人情報を扱うシステムと同様にセキュリティを高めていくべきである。

安心・安全を目指す東芝のセキュリティ技術

図5は安心を縦軸に安全を横軸にとったマトリックスである。IT(情報技術)社会では，利便性を追求するうちに危険な状況に陥り，その危険に気づかないことがしばしばある。その状態がマトリックスの左上“虚の安心”状態である。個人情報の漏えい事件・事故，情報システムのウィルス感染やサイバーアタックの報道は，そのような危険があることを社会に警告している(マトリックス上の矢印A“可視化”に相当)。更に個人情報保護法は，マトリックス上の矢印B“安全性確保”の対応を社会に求めている。そして，東芝グループの情報セキュリティ技術は，安全を可視化した図5右上の“実の安心”を目指している。安全を確保し確認できることで，人々が安心して活動できる社会の実現を図る。

東芝グループ130周年記念サイトのメッセージ[6]は「2005年，130年目を迎える東芝グループのテーマは“驚きと感動”，“安心と安全”(**図6**)，“快適”を世界に発信すること。その実現のため，私たちは全力を挙げて取り組んでいきます。」と結んでいる。東芝グループは，安心・安全な社会と生活の実現に向けて，全力を挙げて取り組んでいる。

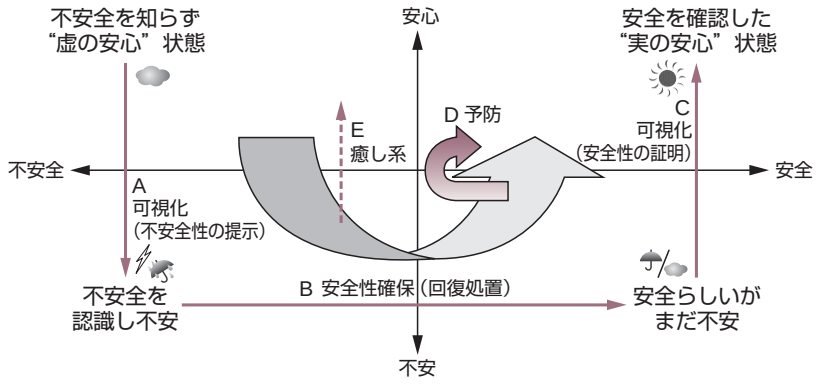


図5．安心・安全マトリックス — 東芝グループの情報セキュリティ技術は，マトリックスの右上の“実の安心”を目指している。

Safety and security matrix

図6．東芝グループ130周年のテーマの一つ“安心と安全” — “安心と安全”を世界に発信するため，東芝グループは全力を挙げて取り組んでいる。

Key phrase of Toshiba Group's 130th anniversary: “Safety and Security”

文　献

(1) 内閣府国民生活局企業課個人情報保護推進室．個人情報の保護に関する法律．＜http://www5.cao.go.jp/seikatsu/kojin/＞，(参照 2005-2-25)．

(2) 経済産業省商務情報政策局情報経済課．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(概要)．＜http://www.meti.go.jp/policy/it_policy/privacy/050114_guideline.pdf＞，(参照 2005-2-25)．

(3) 経済産業省．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．＜http://www.meti.go.jp/policy/it_policy/privacy/privacy.htm＞，(参照 2005-2-25)．

(4) (株)東芝．情報セキュリティおよび個人情報保護の対応強化に向けた新組織の発足について．＜http://www.toshiba.co.jp/about/press/2004_09/pr_j2201.htm＞，(参照 2005-2-25)．

(5) 東芝ソリューション(株)，「個人情報保護法対応基準」制定 様々な業種・業務に向けて適合ソリューションを順次リリース．＜http://www.toshiba-sol.co.jp/ccc/news/detail/041019-2.htm＞，(参照 2005-2-25)．

(6) (株)東芝．東芝グループ130周年記念サイトメッセージ．＜http://www.toshiba.co.jp/130/＞，(参照 2005-2-25)．

由良　浩司
YURA Koji

東芝ソリューション(株) SI技術開発センター 戦略企画担当参事。情報セキュリティ技術の応用製品の開発に従事。電子情報通信学会会員。

Toshiba Solutions Corp.

新保　　淳
SHIMBO Atsushi

研究開発センター コンピュータ・ネットワークラボラトリー主任研究員。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会会員。

Computer & Network Systems Lab.