堅固な基盤技術で俊敏に対応

情報セキュリティ技術は，情報システムへの脅威に対する対策技術であり，システムの信頼性や災害対策まで含めることもありますが，狭義には，悪意の人間からシステムを守るための技術を指します。

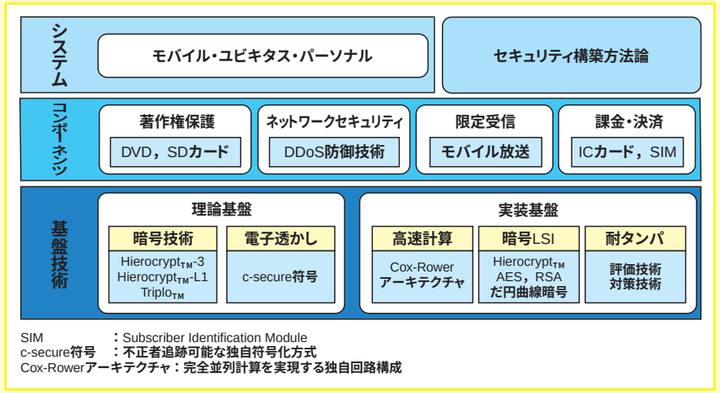
情報セキュリティ技術に限らず，一般に工学では，カスタマーやユーザーと呼ばれる人間を想定して技術開発しますが，能動的に技術の裏をかこうとする悪意の人間を想定するのは，情報セキュリティ技術特有の問題設定です。

■技術体系

情報セキュリティ技術は**図1**に示すように様々な技術要素から成っていますが，ベースとなるのは理論基盤と実装基盤です。このうち，理論基盤では暗号技術と電子透かし技術が特に重要です。実装基盤は暗号をより速く，よりコンパクトに，解析困難な形で実装するための技術であり，高速計算技術，暗号LSIコア，耐タンパ技術が含まれます。

コンポーネントやミドルウェアのレイヤでは，著作権保護，ネットワークセキュリティ，限定受信，課金・決済に注力しています。これらを組み合わせて様々なシステムが構築されますが，効率よく安全なシステムを構築するには，見通しの良い方法論が必要です。

ここではこれらの中から，最近の成果を紹介します。



SIM　：Subscriber Identification Module
c-secure符号　：不正者追跡可能な独自符号化方式
Cox-Rowerアーキテクチャ：完全並列計算を実現する独自回路構成

図1．情報セキュリティ技術の体系　当社が取り組んでいる情報セキュリティ技術の課題をベースに体系としてまとめたものです。

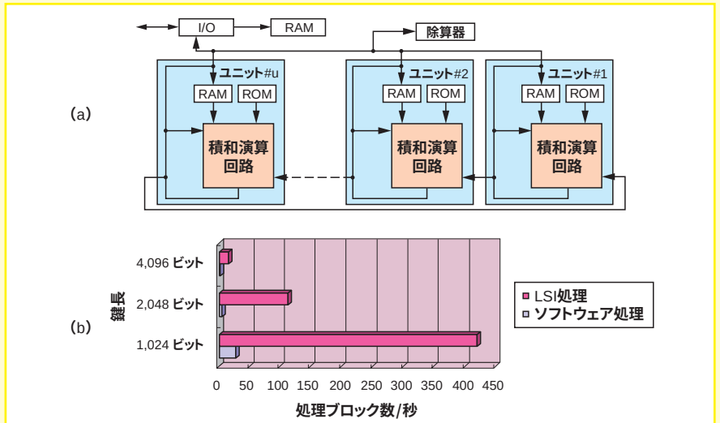


図2．Cox-Rowerアーキテクチャによる高速RSA暗号処理　剰余演算系（Residue Number System）を用いて複数の演算ユニットを同時並列に動作させることで高速処理を実現しています（a）。（b）はソフトウェアとの処理時間比較で，10倍以上の高速化を実現しています。

■共通鍵ブロック暗号Hierocrypt™-3

これは，128ビットブロックで，256ビット鍵までサポートする次世代の共通鍵暗号アルゴリズムです。暗号は安全性と処理性能で評価されますが，Hierocrypt™-3はもっとも汎用性が高く，強力な解読方法である差分解読法と線形解読法に対して，安全性が証明されているという著しい特長を持ちます。またハードウェア，ソフトウェアのいずれでも優れた性能を実現します。

専門家による権威ある暗号評価報告（CRYPTRECレポート）でも高い評価を得ています。

■暗号LSIと耐タンパ技術

暗号はソフトウェア実装されるだけでなく，回路実装されシステムLSIに組み込んで利用される機会が増えています。そのためにHierocrypt™をはじめRSA（Rivest-Shamir-Adleman）暗号，AES（Advanced Encryption Standard）など主要な暗号LSIのコアを開発してコンポーネント化しました。これらを携帯電話，通信用LSI，ICカード，情報家電など様々な用途に適用していきます。

コアの設計にあたっては，独自の並列計算法やコンポーネントの再利用などの技術を駆使することにより，各々の用途に適した特性を実現しました（**図2**）。また，チップを解析されてもLSI内の暗号の鍵が漏えいすることを防止する耐タンパ技術が重要であり，対策と評価技術を研究しています。

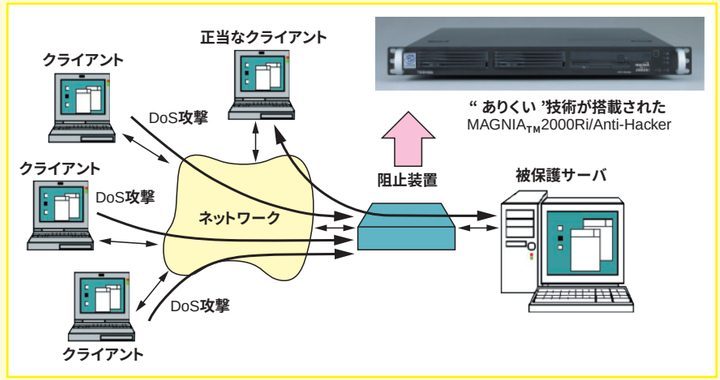
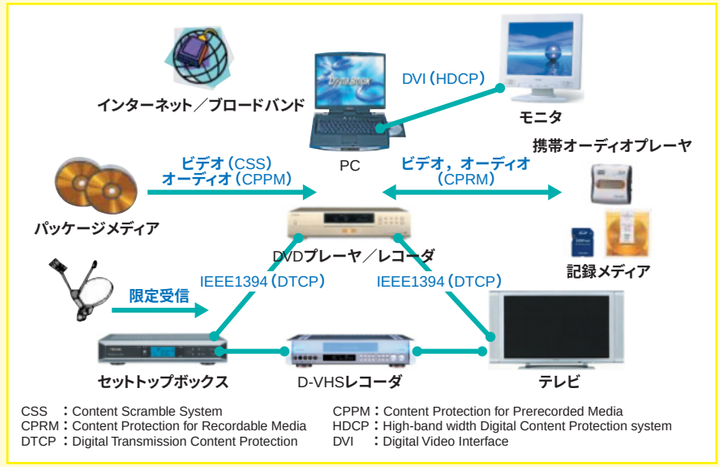


図3．DDoS攻撃防止技術“ ありくい ”　DDoS攻撃を攻撃パターンの特徴により検出して，サーバへの過負荷を防止することができます。



CSS　：Content Scramble System
CPRM：Content Protection for Recordable Media
DTCP　：Digital Transmission Content Protection
CPPM：Content Protection for Prerecorded Media
HDCP：High-band width Digital Content Protection system
DVI　：Digital Video Interface

図4．著作権保護技術　著作権保護技術が，コンテンツの流通を加速します。CSSなど（　）内の記号は，いずれも該当する機器間のコンテンツに対する著作権保護業界規格の略称です。

■DDoS攻撃防止技術

ネットワークを介して複数地点からサーバに多数のアクセスを行い，その機能をまひさせてしまう不正が起こっています。これをDDoS（Distributed Denial of Service）攻撃と呼びます。DDoS攻撃を検出してサーバに過度の負荷がかからないようにすることで，攻撃を回避する技術を開発し“ ありくい ”と名づけました。ありくい技術は当社のインターネットアプライアンスサーバ（MAGNIA™ 2000Ri/Anti-Hacker）に搭載されています（**図3**）。

■著作権保護技術

DVDをはじめとするデジタル記録システムの普及と通信のブロードバンド化で，映画や音楽などコンテンツの不正なコピーを防止する著作権保護技術の開発が重要となっています。DVDやオーディオ機器の分野では，メーカーとコンテンツホルダーが参加して業界規格が作られています。当社は他社と連携して規格の枠組みづくりに貢献するとともに，IEEE（米国電気電子技術者協会）1394バスの機器認証やSDカードの著作権保護メカニズム提案などで技術をリードしています（**図4**）。

■俊敏なシステム開発に向けて

冒頭で述べたように，情報セキュリティは悪意の人間を相手にする技術です。攻撃者は様々な手段を用いてシステムを攻撃しようとします。しかし，本質的に新しい攻撃法が出現することはまれであり，知識を蓄積し必要十分な対策をとることが大切です。

現在，当社ではISO（国際標準化機構）15408「セキュリティ評価基準」の枠組みをベースに，安全なシステムを構築する方法論を開発中です。これは社内技術者が経験的に蓄えた暗黙知を形式知化して，システム開発を加速することを狙うものです。俊敏なセキュリティシステム開発によって，お客さまによりいっそうの満足と安心を提供していきたいと考えています。

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
川村　信一