feature article

社会イノベーションを支える先進セキュリティ技術

Hitachi's Advanced Security Technologies for Social Innovation

洲崎 誠一 Seiichi Susaki
福澤 寧子 Yasuko Fukuzawa
藤井 康広 Yasuhiro Fujii
仲小路 博史 Hirofumi Nakakoji

今後進展が予想される社会インフラと情報システムとの融合や，クラウドコンピューティングに代表される新たな技術潮流の浸透は，これまでの社会環境，事業環境を大きく変える可能性を有している。しかし，一方でそのような変化は，新たなリスクを生み出す危険性をはらんでおり，適切なセキュリティ対策がこれまで以上に重要なものになっていくと考えられる。日立グループは，人々が安心して生活できる社会を実現することを目的に，先進セキュリティ技術の研究開発に取り組み，信頼性・安全性の高い製品・システムを提案している。

1. はじめに

ITの普及・進展とビジネス利用の拡大に伴い，それまで防衛や警察など限られた分野でのみ利用されてきたセキュリティ技術が，より一般的な技術へと変貌（ぼう）を遂げ，さまざまな事業領域でその利用が進んでいる。

一方で，コンピュータやネットワークといったITに依存したビジネスが増えたため，セキュリティ脅威も変質してきており，いわゆる愉快犯的なものから金銭を目的とした犯罪へと目的が明確に変化し，巧妙な不正が増えるなど対策の実施が困難になってきている。

例えば，フィッシングやトロイの木馬，ウイルスなどによって個人情報を盗み出し，銀行口座から勝手に資金移動したり，ショッピングサイトで他人のクレジットカードで買い物したりするなどといった不正が日々発生している。また，情報漏洩（えい）事故を起こしたことによってブランドが棄損され，ビジネス機会が著しく減少した企業も多く，それらのリスクをいかに軽減するかということが重要な課題となっている。

社会インフラと情報システムの融合や，クラウドコンピューティングに代表される新たな技術潮流の浸透など，今後も社会環境，事業環境が大きく変化する中で，セキュリティ技術が果たすべき役割はこれまで以上に大きいと考えられる。

ここでは，安全・安心な社会を実現するため，国からの委託研究として日立グループが取り組んでいる「次世代暗号技術」，「来歴管理技術」，および「P2P（Peer to Peer）を介した情報漏洩への対策技術」について述べる（**図1**参照）。

2. 次世代暗号技術

まず，情報セキュリティを支える暗号技術の一つであるハッシュ関数について，次世代国際標準に向けた取り組みを述べる。

2.1 ハッシュ関数

電子政府やオンラインバンキングなどのシステムでは，ネットワークを介して送受信される情報を保護したり，端末・ユーザーを認証したりするうえで，暗号技術が重要な役割を果たしている。ハッシュ関数とはそのような暗号技術の一つであり，デジタル情報を圧縮して特徴値（ハッシュ値）を算出する関数である。このハッシュ値はデータの指紋とも呼ばれており，異なるデータから算出されたハッシュ値が一致する可能性はきわめて低く，また，元の情報がわずかでも変わるとハッシュ値が大きく異なるといった性質を持っている。このようにハッシュ値の意図的な操作が困難なことから，ハッシュ関数は，不可抗力的なデータ破損だけでなく，悪意をもった第三者による意図的なデータ改ざんも検出可能であり，データの真正性確認手段として幅広く利用されている。

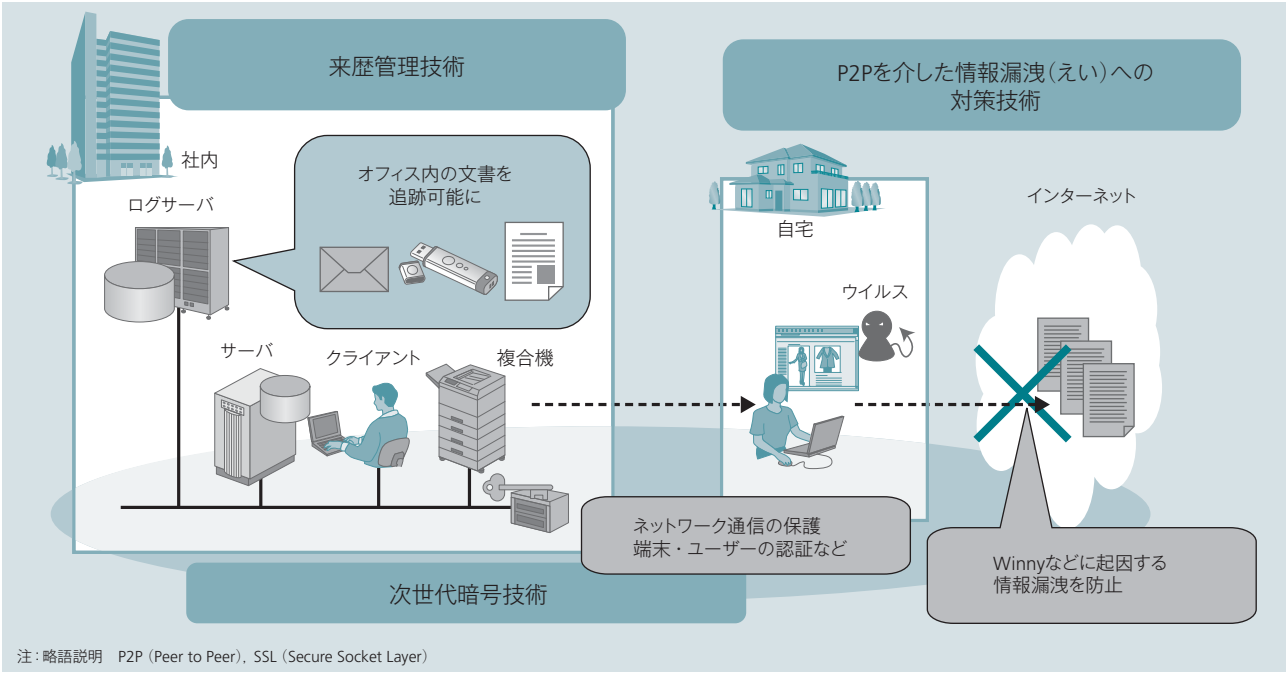
安全性の観点からハッシュ関数が満足すべき要件を以下に示す。

(1) 衝突困難性

同じハッシュ値を出力する二つの入力値を求めることが困難である。

(2) 原像計算困難性

あるハッシュ値に対して，そのハッシュ値を出力するよ



注：略語説明　P2P（Peer to Peer），SSL（Secure Socket Layer）

図1　安全・安心な社会を実現する日立グループの先進セキュリティ技術

「次世代暗号技術」は，SSLなど暗号通信基盤に，「来歴管理技術」はオフィス内の情報漏洩対策に，「P2Pを介した情報漏洩への対策技術」はオフィス外でのWinnyなどに起因する情報漏洩の対策にそれぞれ利用できる。

うな入力値を求めることが困難である。

(3) 第2原像計算困難性

ある入力値に対して，その結果であるハッシュ値と同じハッシュ値を出力する入力値を求めることが困難である。

2.2　次世代標準ハッシュ関数の動向

現在，最も普及しているハッシュ関数は，160ビット長のハッシュ値を出力するSHA-1（Secure Hash Algorithm-1）[1)]と呼ばれるものである。しかし，このSHA-1は，ある種の入力に対して衝突困難性を満たさないという脆（ぜい）弱性が2005年に発見され，期待される安全性を確保できないことが明らかになった。

そのようなSHA-1の急激な安全性低下を受け，NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は，SHA-1を拡張して256～512ビット長のハッシュ値を出力するようにしたSHA-2[1)]を2010年以降利用することに決定し，さらに次世代の標準ハッシュ関数を選定するための「次世代ハッシュ関数コンペティション」（以下，SHA-3コンペと記す。）を2007年11月に開始した[2)]。

SHA-3コンペは，1997年に行われた標準ブロック暗号を選定するAES（Advanced Encryption Standard）コンペティションに続くもので，このコンペティションで選定されたハッシュ関数は，AESと同様に事実上の世界標準として，あらゆる情報システムに利用されるものと予想される。

2.3　日立製作所の取り組み

日立製作所は2004年からハッシュ関数の研究開発に取り組んできており，SHA-3コンペへの提案に向けて，以下の二つのアルゴリズムを開発した。

(1) Lesamnta（レザンタ）

「Lesamnta」は，独立行政法人情報通信研究機構委託研究「次世代ハッシュ関数の研究開発」において，福井大学，神戸大学と共同で開発したハッシュ関数である。Lesamntaでは，一定サイズのデータブロックごとにデータ攪拌（かくはん）処理と圧縮処理とを行うといった，SHA-1でも用いられている従来のハッシュ関数の設計思想を踏襲している。これまで取り組んできたブロック暗号の開発で得られた知見を最大限に活用しており，SHA-1に対する既存の攻撃に対して耐性のある高い安全性を有したアルゴリズムとなっている。

また，実装面では，特に8ビットCPU（Central Processing Unit）上での軽量実装と，64ビットCPU上での高速実装に特徴がある。さらに，標準ブロック暗号であるAESが利用する命令セットアーキテクチャと共通化することで，AES命令が標準搭載される次期CPU上での高速性をねらっている点も特徴である。

(2) Luffa（ルッファ）

「Luffa」は，ベルギーのルーヴァン・カトリック大学と共同で開発したハッシュ関数である。Luffaでは，一定サイズのデータブロックごとにデータ攪拌処理と圧縮処理とを行うという従来の設計思想ではなく，より高速なハッシュ関数を実現するために，最後のデータブロックの前ま

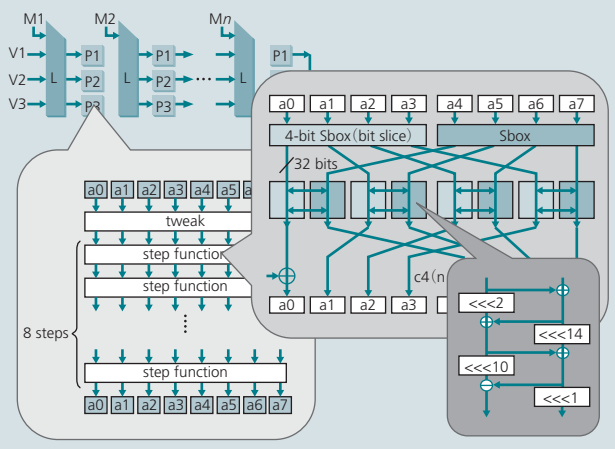


図2　Luffaの詳細構造
ステップ関数の段数大幅削減（従来の$\frac{1}{3}$）と内部状態の拡大（従来の3倍）により，安全性と高速処理とを両立している。

では，データブロックごとにデータ攪拌処理と中間的な圧縮処理（従来の$\frac{1}{3}$程度の圧縮処理）を行い，最後のデータブロックを入力したときだけ最終圧縮処理を行うという新たな設計思想を採用した。この設計思想に基づくハッシュ関数の構成方法は「スポンジ型」と呼ばれており，データブロックごとの処理負荷を小さくし，効率的にデータ圧縮を行うことが可能である。

さらに，Luffaでは，ISO（International Organization for Standardization）で国際標準化済みのストリーム暗号「MUGI」などで培った安全性・高速性・小規模実装に関する技術やノウハウを適用している。また，実装面では，高速処理性と軽量性を兼ね備えたビットスライス型SPN（Substitution Permutation Network）構造を採用することで，ハードウェアでの世界最高クラスの高速性を実現した（**図2**参照）。

2.4　SHA-3コンペの現状

日立製作所は2008年10月，SHA-3コンペに応募し，LuffaとLesamntaを提案した。NISTは，世界中から応募された64方式のアルゴリズムの中から，日立製作所の2方式を含む51方式を次世代標準ハッシュ関数の候補として認定し，SHA-3コンペの第一次選考が行われた。

以来，8か月間にわたって行われた第一次選考では，世界中の暗号研究者が候補51方式の安全性を評価する一方，開発者がアルゴリズムの改定案を提出するなど，オープンな場で熱心な議論が繰り広げられた。この世界中から寄せられた多くの評価結果を踏まえ，NISTは，2009年7月24日に，51方式の中から安全性，高速性の面で優れた14方式を次世代標準ハッシュ関数の第二次選考に進む候補として選定・発表した。日本からの応募では唯一Luffaがこの14方式の中に選ばれた[3]。

第二次選考に進む14方式は，いずれも安全性，実装性などにおいて優れた特性を有しているハッシュ関数である。今後は，2010年夏ごろに最終候補となる5方式が選出され，さらに2年間かけて次世代標準ハッシュ関数SHA-3が決定される予定である。

2.5　今後の展開

今回のSHA-3コンペの第一次選考において，安全性に対する新しい評価手法が開発されるなど技術的に大きな進展が見られた。日立製作所は，時代が進むにつれて，ますます高度化する暗号技術の先端を担うべく，安全性だけでなく，高速性や実装性などあらゆる面から次世代暗号技術に関する研究を推し進め，社会インフラにおける安全・安心の実現に貢献していく。

3.　来歴管理技術

次に，オフィス内での情報漏洩対策に利用される「来歴管理技術」について述べる。来歴管理技術とはログ管理技術の一種であり，転々流通する電子文書および紙文書の利用履歴を収集し，情報漏洩が発生したときに，漏洩元の特定を容易にするものである。以下では，まず従来の情報漏洩対策とその問題点を明らかにし，来歴管理技術の特徴について述べる。

3.1　従来の情報漏洩対策とその問題点

企業内部の機密情報の漏洩対策として，これまでさまざまなセキュリティ製品がリリースされてきた。具体的には，PCなどIT機器の操作ログを収集／管理する製品，可搬媒体への書き込みや印刷を制御する製品，ファイルやディスクを暗号化・アクセス制御する製品などがある。情報漏洩対策製品の市場規模は2008年度時点で300億円程度であり，2013年度には400億円程度に成長していくと予想されている[4]。

これらの製品を利用することで，可搬媒体による機密情報の持ち出しなどといった漏洩事故は確実に減少した。しかしその反面，これらの製品ではカバーできない種類の事故が顕在化してきた。具体的には以下の二つである。

(1) 紙媒体の漏洩

暗号化やアクセス制御など，電子文書に対する情報漏洩対策は進んでいるが，紙文書に対する情報漏洩対策は遅れているのが現状である。その結果，情報漏洩事故全体に占める紙媒体経由での漏洩の割合は年々増加している。2007年度には紙媒体経由の事故が約59.5%に達し，損害賠償額は約1,884億円となった[5]。特に，一度に10万人以上の顧客情報が持ち出された事故が2008年度だけで11件（可搬媒体による持ち出しは1件のみ）あり，紙媒体であっ

ても大量の情報漏洩の危険性は否定できないと言える。

(2) 情報漏洩事故後の対策の遅れによる二次被害

顧客情報などといった機密情報にアクセス制御を施して，特定の権限を持つ管理者しかアクセスできないようにしたとしても，その管理者自身が正規にアクセスした後，外部に持ち出して第三者に転売するなどといった不正行為は防止できない。実際に金融機関や保険会社など，個人情報を多く扱う業種からのこのような漏洩事故が多発している。このようなケースでは，漏洩事故後に早急に原因を究明し，信用失墜や風評被害などといった二次被害を防止することが企業にとって重要である。

漏洩元の特定方法として，現状では，PCの操作履歴やメールサーバのログなど，散在しているさまざまなログ情報を人手で解析することとなるが，それらの作業はきわめて手間がかかるものであり，ミスや漏れが生じる可能性も高い。

以上のような，従来製品では対策が難しい課題を解決することを目的に，来歴管理技術を開発した。

3.2 来歴管理技術の特長

来歴管理技術は，総務省委託研究「情報の来歴管理等の高度化・容易化に関する研究開発」において研究開発を行ってきたもので，既存のログ管理製品と比較して以下の特長を有する。

(1) さまざまな種類のメディアに対応

情報漏洩事故が発生した場合に，漏洩元の特定などにかかる手間をできるだけ削減し，二次被害の防止に向けて迅速に対応できるようにするため，来歴管理技術では，PCやサーバに格納されている電子文書に対する操作ログだけではなく，メールの送受信ログ，可搬媒体の読み書きログ，印刷ログ，さらには複合機の操作ログなどを関連づけながら一元的に管理している。これにより，メディアをまたがった迅速な追跡調査が可能である。特に，紙文書に関しては，日立INSソフトウェア株式会社が「電子透かしプリントソリューションe-紙紋II」[6]として製品化した「二値透かし」技術をベースに，複合機やシュレッダーとも連携し，紙一枚一枚にIDを付与することで，どの紙が印刷，複写，スキャン，廃棄されたかを管理可能としている。

さらに，メール送信，可搬媒体書き出しや印刷といった電子文書の持ち出し時に，ログを収集するだけではなく電子文書のテキスト情報もあわせて収集することで，電子文書・紙文書ログの全文検索も可能となっている。

(2) 情報の追跡が容易

さまざまなログを一元管理した場合，ログが膨大になりやすいが，来歴管理技術では文書操作に関するログだけを選別して管理するため，他のログ収集／管理製品と比較してログの容量を抑えることができる。例えば，ファイルを新規作成しただけで，ファイルシステムのイベントログは20個近く発生するが，これを一つの新規作成ログにまとめる，といった工夫を施している。

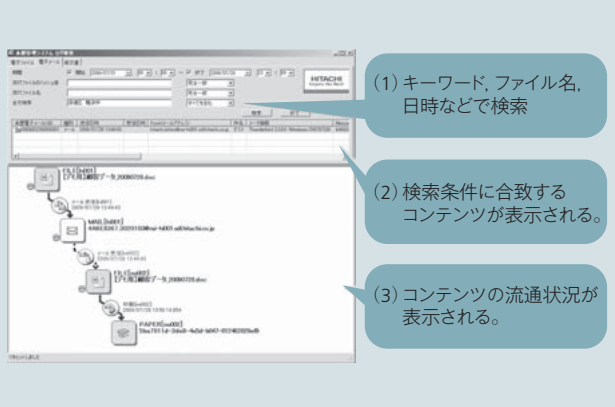


図3 来歴検索のイメージ
転々流通する電子文書および紙文書の利用履歴を収集し，情報漏洩が発生したときに，漏洩元の特定を容易にする。

また，他製品では，検索条件にヒットするログ一覧が表示されるだけ，もしくは簡易的なトレース機能を設けているだけなので，ファイル追跡が困難であるが，来歴管理技術では，検索結果がグラフィカルに表示され，電子文書や紙文書を正確かつ直感的に追跡できるようにしている（図3参照）。特に，ファイル圧縮など，操作元ファイルが複数になる場合にファイルを正しくトレースできる機能は業界初である。

3.3 今後の展開

企業内部の機密情報の漏洩対策としてさまざまなセキュリティ製品がリリースされているが，これら既存製品では対応が難しい紙文書の漏洩や，情報漏洩事故後の対策の遅れによる二次被害などが顕在化している。さまざまな業界にヒアリングし，これらの問題が生じている顧客をいち早く見つけ出すことで，来歴管理技術の早期製品化を進めていく。

4. P2Pを介した情報漏洩への対策技術

最後に，Winnyなどを悪用したウイルスに起因する情報漏洩の対策技術について述べる。

4.1 背景

2003年以降，Winny，ShareなどのP2Pファイル共有ソフトウェア（以下，P2Pソフトと記す。）を悪用したウイルスに起因する情報漏洩事故が多数発生し，いまだに鎮静化の兆しが見えない。特に，個人情報取扱事業者の業務にかかわる範疇（ちゅう）で問題が起きた場合，企業・組織，

そして経営トップの監督責任が問われることとなる。WinnyやShareのような管理者不在のファイル共有P2Pネットワーク（以下，P2Pネットワークと記す。）に流出した情報は，不特定多数の利用者間で増殖しながら広がっていくため，事後にそれらの情報を回収することが事実上不可能な状況にある。

また，世界的にも，誤操作による情報漏洩や著作物ダウンロードによる著作権侵害，大容量トラフィックによるISP（Internet Services Provider）回線の逼（ひっ）迫など，P2P通信自体が社会的問題になっており，P2P通信の制御技術に対する期待が高まっている。

4.2 P2P通信の制御に向けた課題

P2Pソフトでは，通信自体の秘匿性を高めるために中継機能を実装していたり，通信内容を隠すためにDiffie-Hellman鍵交換を利用した本格的な暗号処理MSE（Message Stream Encryption）を実装していたり，サービスポートを固定せず，通信ごとに変更可能とする機能を持っていたりするため，ある通信がP2P通信であるかどうかを特定することすら困難な状況にある。そのため，ファイアウォールや侵入者検知システム（IDS：Intrusion Detection System）などを用いたセキュリティ対策では，十分な効果が望めない。

4.3 情報漏洩対策システムのアーキテクチャ

以上のような課題に対し，総務省委託研究「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」において，P2Pソフトを介して発生している情報漏洩の対策技術（以下，情報漏洩対策システムと記す。）の研究開発を推進している。

情報漏洩対策システムは，通信事業者が運用し，P2P通信の検知と制御とを行うことを想定したものであり，(1) 大容量トラフィックを検知部が持つ複数の検知モジュールに分配する観測部，(2) 分配されたトラフィックを検査してP2P通信である可能性が高い通信を選択する検知部，(3) 検知結果からP2P通信であるか否かを判定する管理部，(4) 判定結果に基づいてP2P通信を制御する制御部から構成されている（**図4**参照）。

以下では，検知部，管理部が具備するプロトコル検知機能，コネクション検知機能についてより具体的に述べる。

4.4 プロトコル検知機能

プロトコル検知機能は，P2Pソフトの通信プロトコルをネットワーク上でリアルタイムに解析し，P2Pソフトが動作しているコンピュータのIPアドレスを特定する機能である。P2Pソフトの中には通信プロトコルの詳細を公開していないものが多いため，この機能の実現にあたっては，利用者が多い七つのP2Pソフト（国内のP2Pソフト利用者の9割以上をカバー）のプロトコルをこの委託研究の中で調査・解析した。

この機能は10Gビット/sのインタフェースを備えたネットワークアプライアンスとして実装しており，大容量トラフィックにも対応可能である。

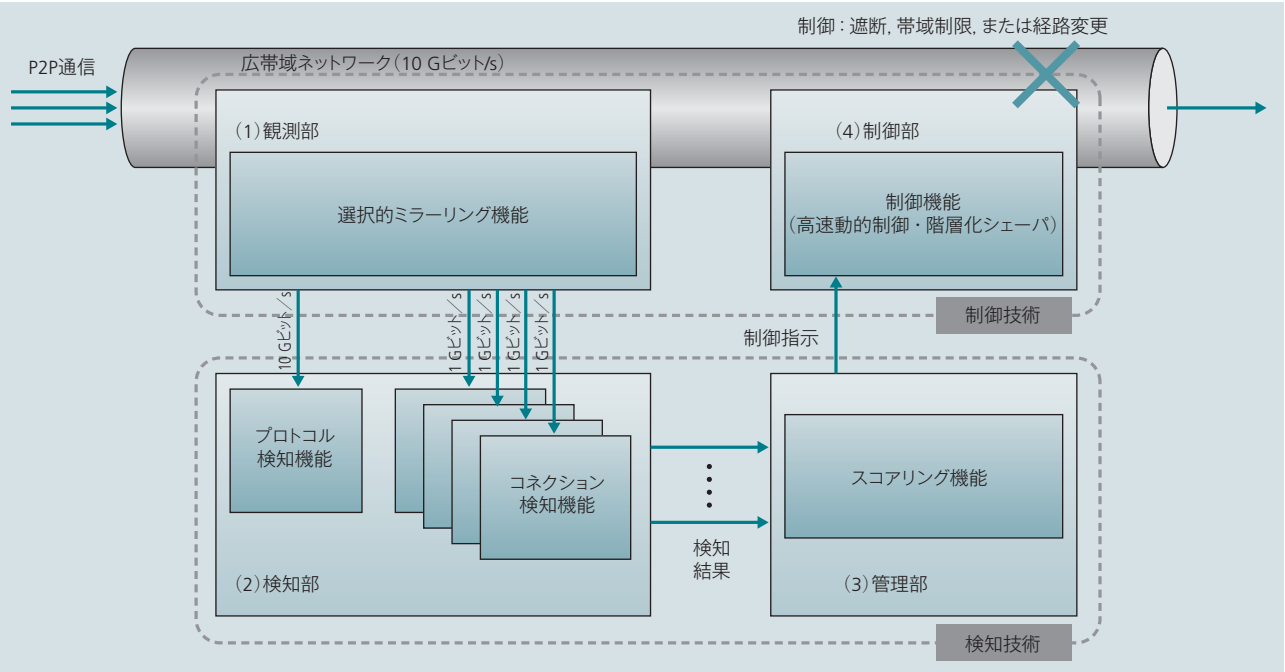


図4 情報漏洩対策システムのアーキテクチャ
大容量トラフィックを分割して複数の検知機能へ配分することにより，広帯域ネットワーク（10 Gビット/s）対応を実現する。

4.5　コネクション検知機能

上述のプロトコル検知機能は，国内で普及している多くのP2Pソフトに対応しているが，それ以外のP2Pソフト，特に今後開発されるであろう新たなP2Pソフトの検知には利用できない。コネクション検知機能は，P2Pソフトの種類に依存しない検知を目的としたもので，メールやWebのようなCS（Client-Server）型の通信と，P2Pソフトを利用したときの通信との挙動の差異に着目した検知方法である。開発したコネクション検知機能の代表的なものを以下に示す。

（1）集約フロー情報に基づく検知方式

この方式は，アラクサラネットワークス株式会社が提案しているフロー統計情報（集約フロー情報）に基づいて，IPアドレス，ポート番号のばらつきを統計的に評価することで，P2P通信か否かを判定するものである。具体的には，サーバとなって他端末からの接続を受けると同時に，クライアントとして複数の他端末へアクセスしているものをP2Pソフト動作端末と判定する。

（2）DNS（Domain Name System）通信履歴に基づく検知方式

一般的なCS型通信では，サーバへのアクセスにホスト名（例えば，www.hitachi.co.jpなど）を用いるため，DNSサーバに事前にアクセスして名前解決を行っている。これに対し，P2P通信では，各P2Pソフト動作端末がIPアドレスによって直接管理されている場合が多いため，事前に名前解決を行わない特徴がある。この特徴に着目し，通信開始時にDNSサーバと通信を行っていないものをP2Pソフト動作端末と判定する。

（3）コネクション確立成功割合に基づく検知方式

一般的なCS型通信では，クライアントがサーバに接続する際に，TCP（Transmission Control Protocol）接続が失敗することはほとんどない。これに対し，P2P通信では，通信相手先の端末が起動していなかったり，IPアドレスが変わっていたりするなどの理由により，TCP接続に失敗する場合が多いという特徴がある。この特徴に着目し，TCP接続の成功割合によってP2Pソフト動作端末か否かを判定する。

以上のようなコネクション検知機能は，新たなP2Pソフトの通信も検知できる可能性を持っているが，その一方で他の通信を誤検知してしまう危険性もはらんでいる。そのため，情報漏洩対策システムでは，複数の検知方式を併用し，その結果に基づいてP2P通信である確率を算出するスコアリング機能を備えている。

4.6　今後の展開

この委託研究の中では，P2Pソフト動作端末を検出するだけでなく，P2Pネットワークを流れるコンテンツの流通制御や，端末上でのウイルス検知技術などについても研究を進めている。今後は，ネットワークにおける対策技術と端末における対策技術を連携させ，より確実な情報漏洩対策システムを構築し，安心なネットワーク利用環境の実現に貢献していく。

5.　おわりに

ここでは，安全・安心な社会を実現するため，国からの委託研究として日立グループが取り組んでいる「次世代暗号技術」，「来歴管理技術」，および「P2Pを介した情報漏洩への対策技術」について述べた。

刻々と新たなセキュリティ問題は発生しており，日立グループは，今後とも先進的なセキュリティ技術の研究開発に邁（まい）進することで社会に貢献していく考えである。

参考文献など

1）NIST：FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 180-3 Secure Hash Standard（2008）
2）NIST.gov - Computer Security Division - , http://csrc.nist.gov/groups/ST/hash/sha-3/index.html
3）NIST.gov - Computer Security Division, Security Resource Center http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/submissions_rnd2.html
4）株式会社富士キメラ総研:2009ネットワークセキュリティビジネス調査総覧（2009）
5）NPO日本ネットワークセキュリティ協会（JNSA）：2008年度個人情報漏洩インシデント調査報告書（2009）
6）日立INSソフトウェア株式会社，電子透かしプリントソリューションe-紙紋II, http://www.hitachi-ins.com/product/ekami/index.html

執筆者紹介

洲崎 誠一
1991年日立製作所入社，システム開発研究所 情報サービス研究センタ 第七部 所属
現在，情報セキュリティの研究開発に従事
博士（工学）

福澤 寧子
1985年日立製作所入社，システム開発研究所 所属
現在，情報セキュリティの研究開発に従事
博士（工学）

藤井 康広
2001年日立製作所入社，システム開発研究所 情報サービス研究センタ 第七部 所属
現在，来歴管理技術の研究開発に従事
博士（理学）

仲小路 博史
2001年日立製作所入社，システム開発研究所 情報サービス研究センタ 第七部 所属
現在，サイバー攻撃対策技術の研究開発に従事