ネットワーク・フォレンジック・システム
MSIESER（Enterprise/Standard/Limited）

ネットワーク利用の情報漏えいの痕跡を記録、情報漏えいの抑止効果、事後対策を強力に推進するシステムであるMSIESERを開発した。MSIESERは、全ての情報を記録し、必要なときに検索、閲覧できる機能を有し、その記録を法廷で証拠とできるほど確かな方法で管理するシステムである。

概　要

MSIESERは、ネットワーク上を流れる通信（LANパケット）を記録し、必要なときに検索、閲覧できるようにするシステムである。ネットワークの不正な利用を抑止するため、ネットワークの利用状況を詳細に記録し、状況を提示するセキュリティ環境構築に最適である。

パケットの解析には高度なネットワーク知識が必要であるが、MSIESERならそうした専門知識を必要とせず、誰もが簡単な操作で通信状況を確認できる。誰が、誰にいつ通信を行ったかの記録のみならず、行き交ったメールやホームページ等のデータを復元することも可能で、強力な抑止力を発揮するとともに問題発生時に迅速な事後解析が可能となる。さらに、MSIESERは,スイッチハブのポートミラー機能やリピータハブを使用してネットワークと接続しパケットを取り込むため、ネットワーク環境に余計な負担をかけず、既存システムへ影響を与えることもない。

MSIESERでは、以下のプロトコルを解析することが可能である。

表1　対応プロトコル

レイヤ	プロトコル
アプリケーション	HTTP，SMTP，POP3*1，FTP*1
プレゼンテーション	
セッション	
トランスポート	TCP
ネットワーク	IP
データリンク	Ethernet

＊1 Standardのみ対応

（注１）　IPv4にのみ対応。
（注２）　VLANには未対応。
（注３）　暗号化通信では、TCP/IP及びETHERヘッダ情報のみ解読可能。

開発の経緯

2002年10月　標準タイプであるStandardを開発し、販売を開始。
2004年７月　機能を特化させた普及タイプであるLimitedを開発し、販売を開始。
2005年１月　大規模システムに対応可能なEnterpriseを開発し、販売を開始。
2007年１月　大容量データの蓄積を可能としたStandardを開発し、販売を開始予定（Limitedは Standardに統合）。

各製品の機能強化、性能向上を継続して実施している。

特　長

Standard、Enterpriseそれぞれの特徴を以下に記述する。

MSIESER Standard

Standardは、パケット取得から解析まで、１装置で構成している。

・ユーザ（端末）数 4,000人程度まで
・smtp，http，ftp，pop3，others（TCP/IP）
・テープバックアップ
・ディスク冗長化（RAID0＋1，RAID5など）
・システム管理、データ閲覧の権限分割

MSIESER Enterprise

Enterpriseは、パケット取得装置、蓄積装置及び解析装置で構成している。

・ユーザ（端末）数 20,000人程度まで
・smtp，http，others（TCP/IP）
・ディスク冗長化（RAID0＋1，RAID5など）
・テープバックアップ可
・記録データを暗号化、改ざん防止機能あり
・システム管理、データ閲覧、ログ監査の権限分割
・NASへの大量蓄積

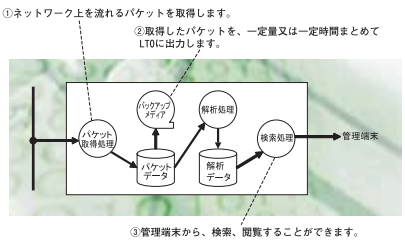


図１　装置構成（Standard）

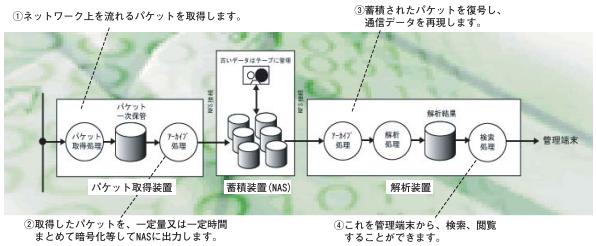


図２　装置構成（Enterprise）

個人情報ファイル検出ツール
すみずみ君

クライアントPC内に保存されている個人情報と思われるデータを検出するツールすみずみ君を開発した。（PCの使用者が個人情報ファイルの存在を把握することにより、教育効果（モラル向上）と漏えいリスクの低減に効果あり。）

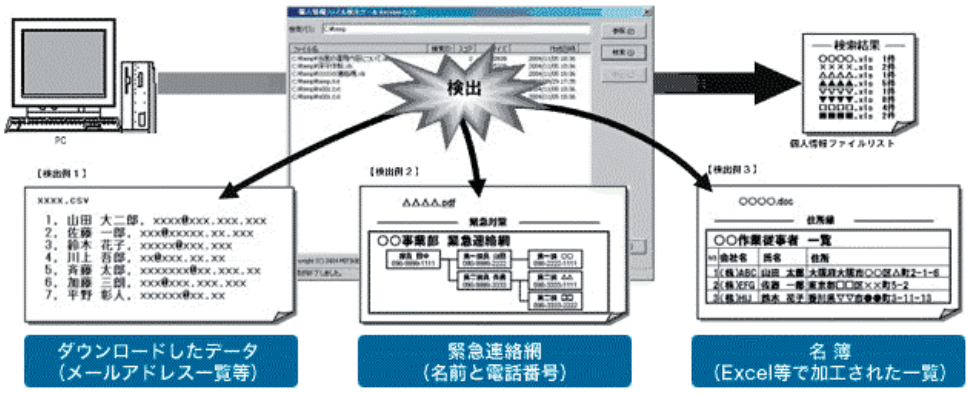
サーバ用ソフト「すみずみ君SV」との連携により、個人情報ファイル検出データの収集・管理が可能である。

すみずみ君の概要

「すみずみ君」は、PCのディスクや媒体に保存されているファイルの中身をすみずみまで検査し、個人情報に該当すると思しきファイルを検出する。検出結果の一覧からファイル内容の閲覧や削除ができる。

人の記憶に頼った調査では限界があり、例えばWEB閲覧の結果として保存されるキャッシュファイル、メールの添付文書を開いたときに作成される一時ファイル、ごみ箱の中のファイル等、利用者も気付かないうちに個人情報ファイルが蓄積し、情報漏えいのリスクが見過ごされていることがある。すみずみ君は、これらの見過ごされた個人情報ファイルを検出し、特に次のような用途において効果を発揮する。

・情報資産の棚卸しツールとして
・持ち出しPC・媒体の安全性チェックとして
・セキュリティ監査・教育ツールとして



すみずみ君SVの概要

「すみずみ君」では、パソコンごとに利用者が検査条件を設定するが、「すみずみ君SV」では、組織のパソコン全体を管理するシステム管理者により、各パソコンで実行される「すみずみ君」の検査条件を統一的に設定することができる。これにより、検査の漏れやバラつきを防ぐことが可能になる。

また、各パソコンの利用者が、システム管理者からの検査指示を受け、「すみずみ君」を実行すると、「すみずみ君ＳＶ」により設定された検査条件で検査が行なわれる。その検査結果は、「すみずみ君」から自動的に「すみずみ君ＳＶ」に通知される。検査の進行状況は、システム管理者が随時確認することができ、検査の未実施者に対する督促が可能となる。

検査が完了し、検査結果がサーバ側に集積されると「すみずみ君SV」は、それをCSV形式のファイルとして出力することができる。CSV形式で出力された集計結果は、EXCELなどにより自由に加工、編集することができ、組織の方針、状況、環境に応じた個人情報管理を行うことができる。

すみずみ君の新機能

「すみずみ君」の次期バージョンでは、以下の新機能が追加となる。

⑴　組織の管理強化のための機能

・任意キーワード設定機能

・強制検査実行機能

⑵　個人の管理強化ための機能

・検出ファイルのドラック&ドロップ機能（暗号化ソフトへドラッグ&ドロップで簡単に暗号化）

・検出結果のソート機能

開発の経緯

2004年コア技術となる「ストリーム高速フィルター（検索エンジン）」の開発（※検索エンジンの開発は、三菱電機㈱情報総研への小口研究依頼による。）

2005年１月　プレス発表、Ver1.0.0リリース

2005年７月　すみずみ君Ver1.2.0リリース、すみずみ君SV Ver1.0.0リリース

2006年２月　Ver1.4.0リリース、すみずみ君SV Ver1.1.0リリース

2006年３月　Ver1.6.0リリース、すみずみ君SV Ver1.2.0リリース

特　長

・個人情報(名簿)検出アルゴリズム搭載！

顧客リスト、緊急連絡網等の名簿に類する個人情報を検出するアルゴリズム（特許出願中）を搭載しており、個人情報に該当すると思われるパターン（苗字と電話番号のパターン、苗字とメールアドレスのパターン等）が含まれている文書ファイルを検出する。

・主要なアプリケーション形式に対応！

MS-Word95/97/98/2000/2002（XP）/2003、MS-Excel95/97/2000/2002（XP）/2003、MS-PowerPoint95/97/2000/2002（XP）/2003、MS-Access2000/2002（mdbファイル）、PDF Acrobat4.0/5.0/6.0、テキスト形式、CSV形式、一太郎V7～V13/2004、OASYSV6/V7/V8/2002、LotusWordPro2001、圧縮ファイル（zip/lha/tar/tgz)、RTFファイルなどに対応している。

・操作は簡単！

フォルダを指定し、検索ボタンをクリックするだけで検索することができ、初心者でも簡単に操作することができる。

電子メールフィルタリング装置
LeakStopper for SMTP

うっかりミスによるメールの誤送信を防止する電子メールフィルタリング装置。

従来のメールフィルタリング製品の基本機能に加え、個人情報漏えい防止機能を標準搭載。個人情報の検査条件がプリセットされていることが最大の特徴。

また、日本語正規表現、同時送信先禁止設定等、他社にない独自の検査条件設定機能を有している。

概　要

「LeakStopper for SMTP」は、基幹ネットワークもしくは部門内ネットワーク内のクライアントPCと既存の送信メールサーバとの間に設置し、クライアントPCから送信されたメールを検査する。

検査の結果、検査条件に該当するメールは一旦保留し、送信者本人／管理者宛に保留の旨を通知する。通知内容を確認後、送信者本人もしくは管理者の操作によりWEB画面から当該メールの送出／削除を行うことができる。保留の通知、送出等の権限は、送信者のみ／管理者のみ／送信者と管理者の両方／等、ポリシーに応じて設定することができる。

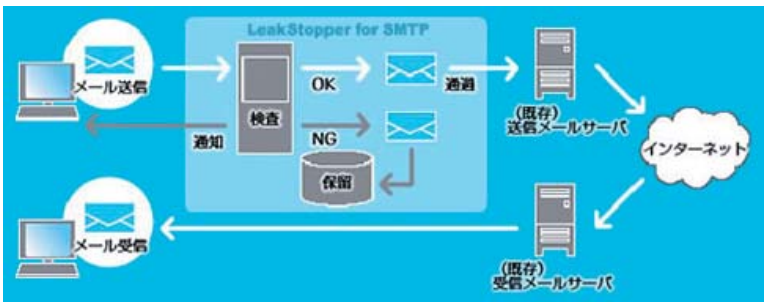


図１　LeakStopper for SMTP設置例

表１　LeakStopper for SMTP主要機能一覧

LeakStopper for SMTP 主要機能		概要
検査機能	個人情報（名簿）漏えい防止機能	個人情報（名簿）らしきデータを含むメールを保留する機能
	検査条件キーワード検査機能	設定した検査条件キーワードを含むメールを保留する機能 検査条件キーワードとして固定文字列、論理式（AND，OR）、正規表現（日本語可）が設定可能
	検査条件添付ファイルタイプ検査機能	設定した検査条件ファイルタイプ（拡張子）のファイルが添付されたメールを保留する機能
	ドメイン外アドレス自己確認機能	検査対象ドメイン以外のアドレスを送信先に含むメールを保留する機能
保留通知機能		検査条件に該当したメールの送信者、管理者宛に保留された旨を通知する機能 通知先は 送信者のみ/管理者のみ/送信者と管理者 に設定可能
保留メール処置機能		保留されたメールの処置（送出または削除）を行う機能 送信者本人に保留メールの処置権限を与える設定も可能
検査結果閲覧機能		設定した検査条件による検査結果を確認する機能（管理者）
保留メール処置履歴閲覧機能		どの保留メールに対して、いつ、どのような処置（送出または削除）が取られたか確認する機能（管理者）
統計情報閲覧機能		設定されている検査条件や、検査条件毎の検査状況を確認する機能（管理者）
ホワイトリスト機能		送信先を、あらかじめ登録されているアドレスのみに制限する機能（管理者）

開発の経緯

2004年　コア技術となる「高性能ストリームデータ検索エンジン」の開発
（※検索エンジンの開発は、三菱電機㈱情報総研への小口研究依頼による。）

2005年２月　プレス発表

2005年５月　LeakStopper for SMTPを開発し、販売を開始。

機能強化、性能向上を継続して実施している。

特　長

従来のメールフィルタリング製品の基本機能（固定文字列＋論理式（AND，OR等）を用いた検査条件による固定文字列の検査機能）に加え、個人情報検出アルゴリズム、日本語正規表現を含むキーワード検査条件、同時送信先検査条件等を用いた多彩な検査条件による検査が可能である。また、「高性能ストリームデータ検索エンジン」により、複雑な検査条件または大規模な検査条件を設定した場合においても高速処理が可能である。

「LeakStopper for SMTP」の導入により、企業機密漏えい防止及び個人情報漏えい防止を目的とした、より効果的なメール監視運用が期待できる。

表２　LeakStopper for SMTP特長

LeakStopper for SMTP 特長	概　要
個人情報（名簿）検出アルゴリズム標準搭載	顧客リスト、緊急連絡網、体制図等の名簿に類する個人情報を検出するアルゴリズム（※特許出願中）を標準搭載
日本語正規表現を用いた柔軟な検査条件の設定が可能	日本語を含む正規表現を使用することにより、表記ゆれ（例：取り扱い注意/取扱注意）のある検査条件の設定が可能
高性能ストリームデータ検索エンジン搭載	高速文字列照合の実現により、通常のメール運用を妨げない迅速な判定処理が可能
同時送信先検査条件の設定が可能	同じ送信内容を宛先により同時送信することを禁止する設定が可能
多彩な添付文書に対応	様々な圧縮形式（lha/zip/tar/tgz）、主要なアプリケーション形式（Word/Excel/PowerPoint/PDF Acrobat/一太郎 等）に対応
自己チェック機能	送信者本人に保留メールの処置権限を与え、管理者の負荷を軽減させる運用も可能
テストモード設定が可能	検査条件に合致しても保留せず、監視のみを行う運用が可能

ネットワークカメラ遠隔モニタリングシステム
SPACESERVER

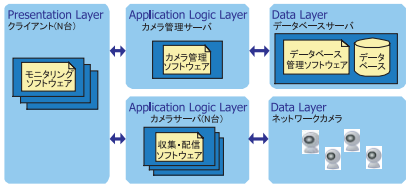
小規模から大規模まで、ニーズに合わせた遠隔モニタリングに対応するネットワークカメラ遠隔モニタリングシステムを開発した。

概　要

・計算機室などの小規模エリアから、ビル全体の広域エリアまで、幅広く遠隔モニタリングを行う事ができる。
・複数メーカのカメラの映像を一元でモニタリングすることができる。
・カメラ台数の拡張も、サーバの増設により柔軟に行うことができる。
・表示画面レイアウトも、お客様のニーズに合わせて自由に変更できる。

SPACESERVERとはIPネットワークで接続された多数かつ多様なカメラの画像録画、画像配信、またカメラ制御を一元で行うネットワークカメラ集中管理システムである。N層モデルを採用し、各ソフトウェアを疎結合とすることで、必要な機能のみを並列化することができ、スケーラビリティを確保することができる。またカメラサーバがカメラ機能の差異を吸収することにより、ユーザはカメラの種類・メーカを意識することなく、モニタリングやカメラ制御を行うことができる。ActiveX※を用いてクライアントを構成したことにより、専用の端末を必要とせず、サーバにアクセスできるPCであれば、Internet Explorer※を用いてモニタリングや制御を行うことができる。録画された画像はカメラサーバに保管し、クライアントからいつでも検索・閲覧することができる。

代表的な構成図



N層モデル概要

特　長

・ネットワークカメラの映像をLAN経由でInternet Exprolerによりモニタリングすることが可能。
・ユーザID、パスワードによりカメラ毎のアクセス制御が可能。

1サーバで100台のカメラをサポート（ネットワーク環境、サーバスペックにより異なる）し、サーバの増設により数台から数百台のカメラ接続が可能。

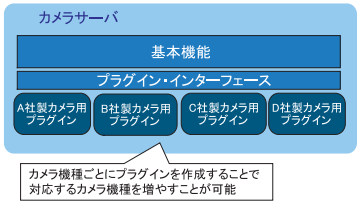
・クライアントPCからパンチ・チルト、ズームなどのカメラ制御が可能。
・プラグイン方式による構成

カメラサーバは下図に示すように基本機能部分と、各カメラ用プラグインで構成される。カメラ・インターフェース・モジュールをプラグイン形式とすることにより、基本機能部分を変更することなく、新しいカメラ機種のサポートを可能とする。

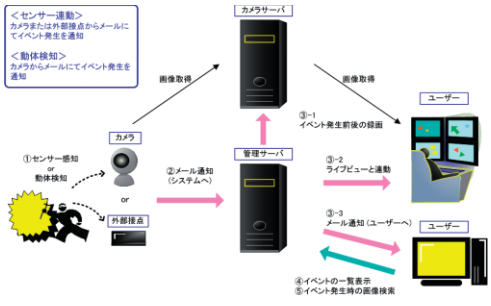
・イベント連動機能により外部センサと連動が可能。

外部の各種センサと連動することができ、それらのイベントをトリガとして、録画や、プリセット移動、ライブ画像配信などを行うことができる。またイベント時の録画はイベント発生前の一定時間の画像も記録することができる。イベント受信部もプラグイン方式にて構成されており、多様な外部機器に対応することが可能である。（標準では特定メーカの接点機器に対応。）

※ActiveX は米国Microsoft Corporationの登録商標です。
※Internet Explorerは米国Microsoft Corporationの登録商標です。



プラグイン方式



イベント発生時のフロー

来訪者向けIDカード即時発行ソフトウェア
COCOPRICO® GATE

顔写真を撮影し、COCO-DATESコード(※)を付与したカードをその場で発行し、入退場管理を行うことのできるシステムを開発した。

概　要

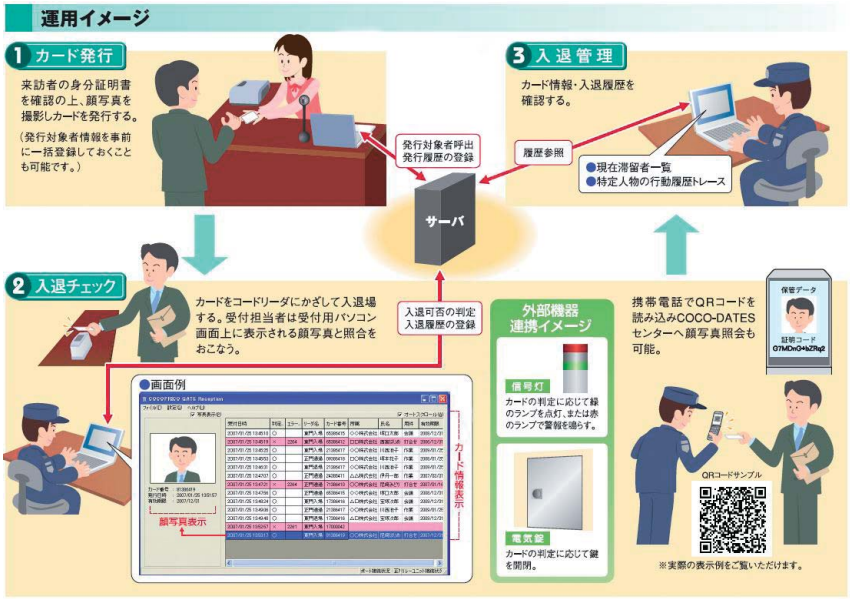
近年のセキュリティ意識の高まりにより、事業所や工場などでの外来者の入退場管理において、従来のバッジと目視による管理ではなく、個人を特定できる管理方法に関するニーズが高まってきている。しかし、そのようなシステムを導入する場合、ICカードによるシステムが一般的であり、初期コストおよびランニングコストは高価になってしまっていた。また依然として目視上は匿名であり、カード持ち帰り対策なども必要である。

COCOPRICOは安価に個人を特定可能な管理を実現したいというニーズに応えるべく開発を行った製品である。

特　長

・紙カードとQRコードを用いた安価な入退場管理システム。
・PCカメラで撮影した写真入りのカードをその場で作成。
・カードは市販のインクジェットプリンタと名刺用紙を使用可能。
・データベースにより、カード発行履歴・入退場履歴を集中管理。
・ユーザが任意にカードレイアウト、デザイン、管理項目を変更可能。
・QRコードリーダによる入退場チェックが可能。
・写真はシステムで管理し、QRコードチェック時に同時に画面にも表示できるため、本人確認が容易。
・COCO-DATESサービスが提供するサーバにも写真を登録可能なため、第三者による信頼性の高い本人証明が可能。

システム構成例



※COCO-DATESコード：三菱電機の位置時間証明情報提供サービス
「COCO-DATES（ココデイツ）」から発行される、位置時間証明情報コード。「COCO-DATES（ココデイツ）」は、三菱電機株式会社の商標です。