# Decision Computer 社 フォレンジック関連製品説明

## 1. E-Detective／Wireless-Detective シリーズの概要

E-Detectiveシリーズは,LAN上の各種インターネットプロトコル準拠のデータをパケットキャプチャし、デコード、再生することによって、コンテンツのフロー監視を行う究極のツールであり、情報漏洩対策を含めたトータル フォレンジック ソリューションです。

E-Detective／Wireless-Detective シリーズ（E-Detective Data Centre を除く）は、LAN 上のデータ トランザクション全てをキャプチャし、キャプチャ データをリアルタイムでプロトコル デコード、再生、表示します。
また、管理機能としては、キーワード・パラメータによる検索、異常通知／警告の発報、CD あるいは外付けストレージへのバックアップ等があります。

このシリーズのうち、E-Detective はワイヤード LAN 環境を対象にし、Wireless Detective はワイヤレス LAN 環境を対象にしたソリューションです。
また、E-Detective Data Centre は、E-Detective／Wireless-Detective 又は他のパケットキャプチャ装置でキャプチャされたデータをオフラインでデコード解析するソリューションです。

E-Detective／Wireless-Detective シリーズの特色としては以下のような点が上げられます。

- LAN 上の各種プロトコルデータのキャプチャ、デコードおよびオリジナルフォーマットへの再生・表示・保存が可能
  対応プロトコル:
  - ✓ Email（POP3・SMTP・IMAP・Webmail）
  - ✓ Instant Messenger/Chat（Yahoo・MSN・ICQ・AOL・QQ）
  - ✓ File Transfer（FTP・P2P）
  - ✓ HTTP（Link・Content・Reconstruct・Download/Upload）
  - ✓ Telnet
  - ✓ Online Games Log
  - ✓ VoIP
  - ✓ Webcam
  - ✓ Video Stream(*) * Wireless-Detective は非対応
- キーワード、パラメータ、類似、グループなどによる検索機能
- キーワード等による異常通知／警告の発報
- 各種レポート作成（統計レポート、チャート、エクセル形式でのインターネット ログ）
- ワイヤレス機器の設置方位、場所の推定(*) * Wireless-Detective のみ対応（指向性アンテナ、あるいは GPS 利用オプション モジュールが別途必要）

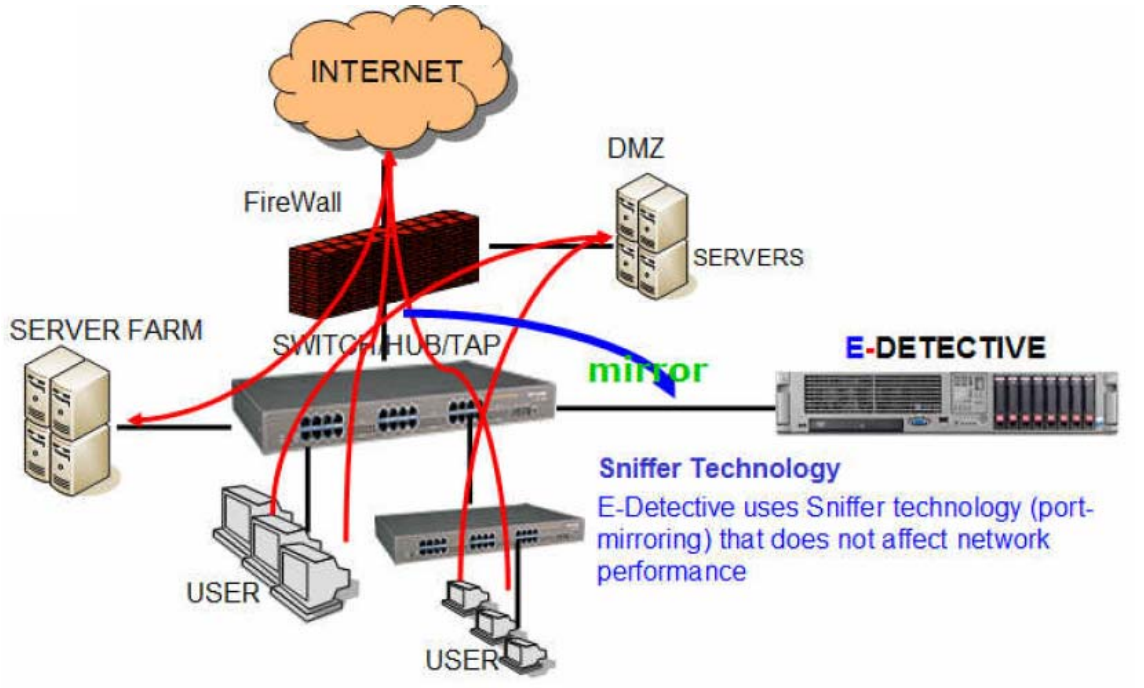
## ２．VoIP-Detective シリーズの概要

VoIP-Detective シリーズは、インターネット上の VoIP セッション（RTS セッション）のキャプチャ、デコード、再生、表示します。また、VoIP 電話の録音、音声再生をするだけではなくコンテンツ全てを記録、バックアップすることができます。

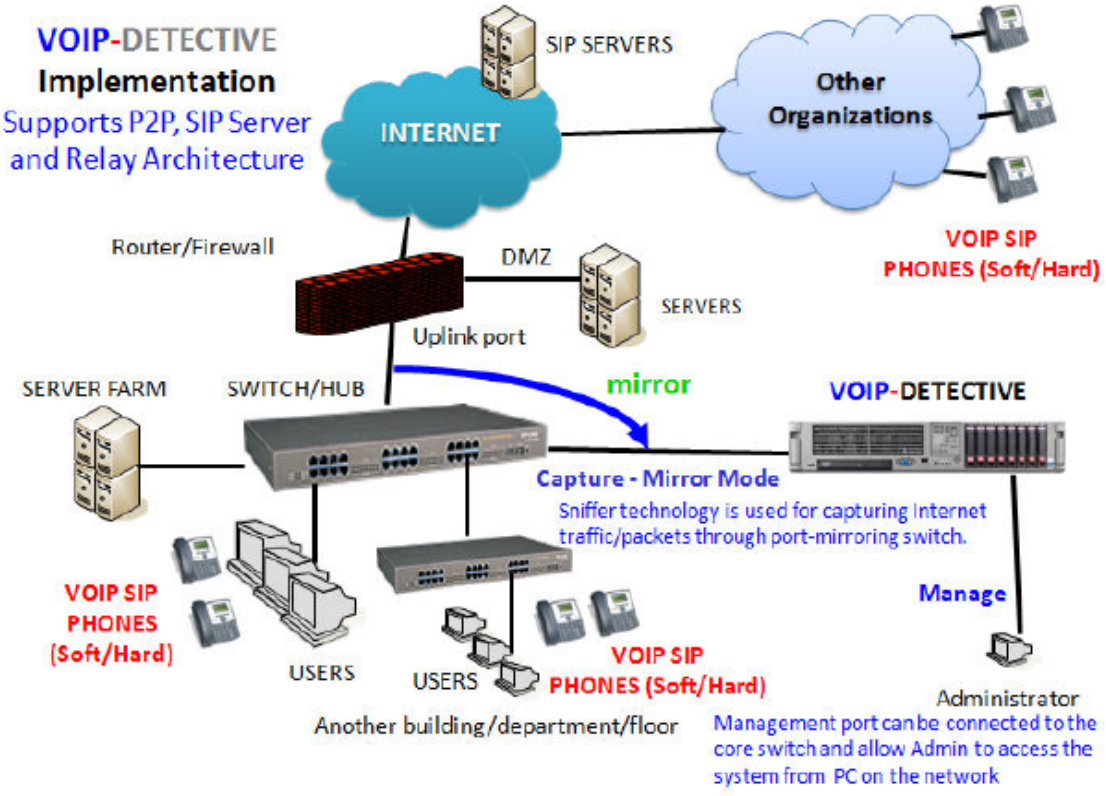
対応プロトコルは、SIP および H.323 であり、対応コーデックは G.729、G.711-a law、G.711-u law、G.723、G.726 および ILBC です。

[概念図]

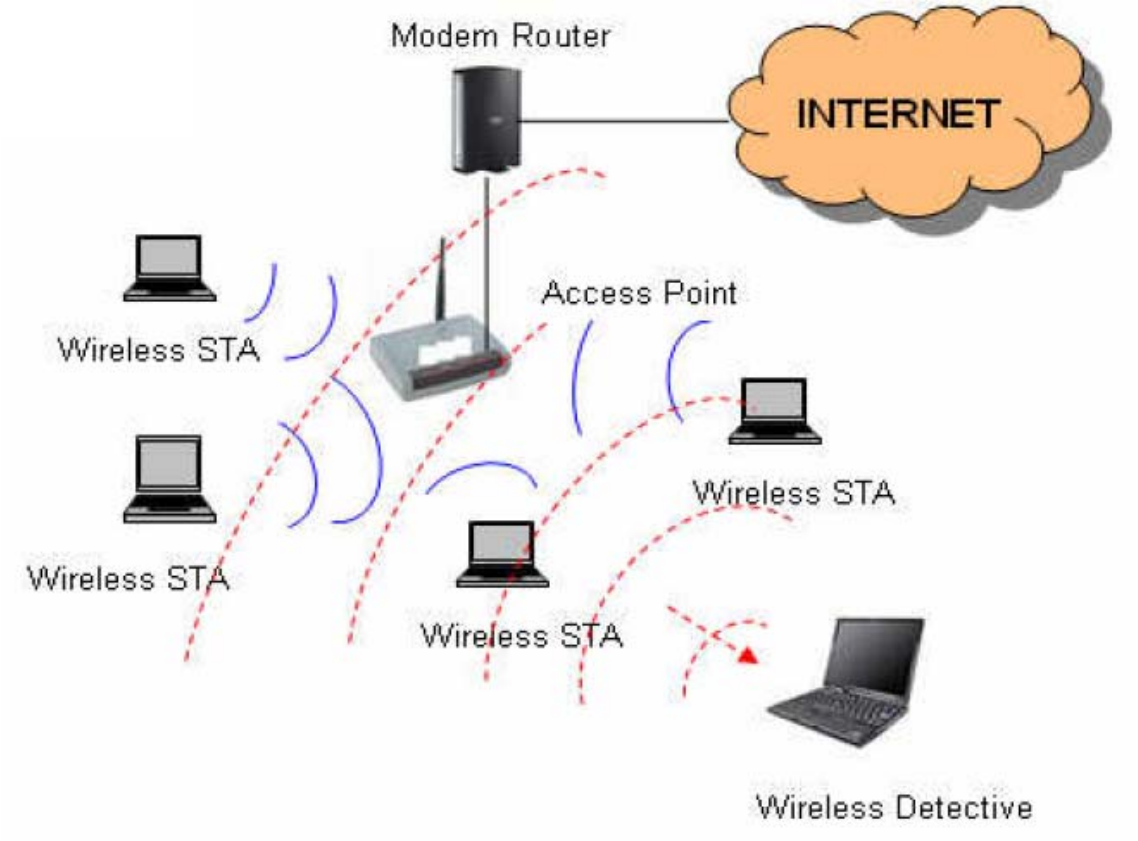
E-Detective Professional　適用例




VoIP-Detective　適用例



Wireless-Detective　適用例




## 3. E-Detective のラインアップ

### 3-1. E-Detective Professional

- スイッチのミラー　ポートで、各種プロトコルデータをオン-ザ-フライでキャプチャし再生
- フルコンテンツ及びインターネット　ログ（アカウント、IP/MAC、送信者/ユーザ、受信者/参加者、タイトル等の情報を含め）を再生

### 3-2. E-Detective Network Supervisor

- スイッチのミラー　ポートで、各種プロトコルデータをオン-ザ-フライでキャプチャし再生
- インターネット　ログ（アカウント、IP/MAC、送信者/ユーザ、受信者/参加者、タイトル等の情報を含め）のみ再生　（再生されたコンテンツは表示せず）

### 3-3. E-Detective Decoding Centre　（EDDC）

- 各種プロトコルデータの解析およびフォレンジック調査における解析作業をジョブ分散をすることが可能
- 各種プロトコルキャプチャ データをオフラインでデコード、再生。サーチ機能、エクスポート/バックアップ機能付きでケースID管理可能なインターネットデータ解析用ソフトウェア

## 4. VoIP-Detective

- VoIP セッション（RTP セッション）のキャプチャ、デコード、再生ソフトウェア
- VoIP 電話の音声再生
- 各種プロトコル（SIP、H323）、各種コーデック（G.729、G.711-a law、G.711-u law、G.723、G.726、ILBC）、VoIP アーキテクチャ（P2P、SIP サーバ、リレイ）に対応

## 5. Wireless-Detective のラインアップ

### 5-1. Wireless-Detective Standard

- 802.11 a/b/g ワイヤレス標準環境のワイヤレス機器（Wi-Fi 可能機器）が対象標準条件下、周囲 100m の範囲をカバー
- 特定 AP/STA の追跡・データ キャプチャやチャンネルごとの追跡・データ キャプチャが可能
- 自動あるいは手動による WEP キー 解読（64、128 および 256-bit）
- 対応するプロトコルは Email（POP3・SMTP・IMAP・Webmail Read & Sent）、Instant Messengers（Yahoo・MSN・ICQ・AOL・QQ・Skype）、File Transfer（FTP・P2P）、HTTP（Link・Content・Reconstruct・Upload/Download）、Telnet、Online Games、VoIP（Yahoo）、Webcam（Yahoo・MSN）
- キーワードによる検索およびパラメータによる検索
- 管理者への email による各種異常通知および警告の発報
- tcpdump（pcap）による外部からの生データのインポートおよびキャプチャした生データあるいは再構築したデータの外部へのエクスポートあるいはバックアップ
- 管理者によるユーザ権限設定
- 管理者による IP およびネットワーク情報の設定が可能
- 特定データ若しくは全てのデータの消去が可能
- 対象 AP/STA の緯度・経度把握のための GPS 利用（オプション）

### 5-2. Wireless-Detective Enhanced

- Wireless-Detective Standard の全ての機能をサポート
- より広い場所的カバー範囲

5-3. Wireless-Detective Extreme

- Wireless-Detective Standard の全ての機能をサポート
- 広域ワイヤレス LAN をカバーし、Distributed System アーキテクチャ ベースの整合性の高い再生を可能にするハイエンド ワイヤレス LAN パケットキャプチャ
- AP/STA 接続禁止機能（ジャミング機能）
- AP/STA の設置方位・位置推定機能（別途、指向性アンテナあるいは GPS 利用オプション モジュールが必要）

## 6. 技術サービス

コアマイクロシステムズより以下のような技術サービスが提供できます。

- 評価用無料ダウンロード
- 評価用アプライアンス貸出
- OEM アプライアンス開発
- 大規模インテグレーション
- 共同開発

## 7. E-Detectiv シリーズ　参考価格

| 名称 | 形式 | 主仕様 | 標準価格 |
|---|---|---|---|
| E-Detective Network Supervisor-50 | AEDS-50 | 50ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Network Supervisor-100 | AEDS-100 | 100ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Network Supervisor-300 | AEDS-300 | 300ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Network Supervisor-1000 | AEDS-1000 | 1000ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Professional-30 | AEDSC-30 | 30ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Professional-50 | AEDSC-50 | 50ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Professional-100 | AEDSC-100 | 100ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Professional-300 | AEDSC-300 | 300ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Professional-500 | AEDSC-500 | 500ユーザまでのソフトウェア　ライセンス | オープン |
| E-Detective Professional-1000 | AEDSC-1000 | 1000ユーザまでのソフトウェア　ライセンス | オープン |

## 8. VoIP-Detectiv シリーズ 参考価格

| 名称 | 形式 | 主仕様 | 標準価格 |
|---|---|---|---|
| VoIP-Detective-50 | AED-VoIP-SS50 | 同時セッション数：50までのソフトウェア ライセンス | オープン |
| VoIP-Detective-100 | AED-VoIP-SS100 | 同時セッション数：100 までのソフトウェア ライセンス | オープン |
| VoIP-Detective-200 | AED-VoIP-SS200 | 同時セッション数：200 までのソフトウェア ライセンス | オープン |
| VoIP-Detective-300 | AED-VoIP-SS300 | 同時セッション数：300 までのソフトウェア ライセンス | オープン |

9. その他の製品についての参考価格は、弊社営業までお問合せください。

電話：050-5558-5410 / 03-5917-6451
email：sales@cmsinc.co.jp

以上