

Ji2 ニュースレター

(フォレンジック / インシデント・レスポンス)

2008 年 12 月号

はじめに

世界的な景気後退で2008年も終わりを告げようとしています。フォレンジック業界は不景気に強い産業ではないかと米国専門家の間ではささやかれています。実際は来年2009年を迎えてみないと分かりませんが、不景気による「裁判案件の増加」や「サイバー犯罪の増加」が現実となればフォレンジック業界やeDiscovery業界にいる我々のようなベンダーは正義の味方？として活躍の場が増えるかも知れません？

12月号の内容

1. 最新ビジネス・ニュース	2
2. テクニカルニュース	4
3. 製品紹介	6
4. アップデート情報	8
5. イベント情報	9

Note: Ji2 ニュースレターは「**フォレンジック**」「**インシデントレスポンス**」「**電子証拠開示 (eDiscovery)**」の各ビジネス分野の日米のパイオニアとして最新ニュースを[ビジネス]と[技術]の2つにフォーカスして発信しております。今後カバーするトピック・キーワードと致しましては、**電子証拠開示技術 (Legal Technology)**、**レビュープラットフォーム (Review Platform)**、**電子証拠取得 (eDiscovery)**、**米国裁判での事例紹介**、**フォレンジック最新技術**などを予定しております。

今後とも、日米発のフォレンジック・インシデント・レスポンス情報を、いち早く日本語でお届けするニュースレターを2ヶ月に一回の割合で、お届けするように努力しております。内容について、ご意見・ご要望などございましたら、ご一報いただければ幸いです。

株式会社 Ji2 とは : 2001 年より米国法人、そして 2007 年 8 月より日本法人を持つ日米ハイブリッド企業。コンピュータ・セキュリティのインシデント対応「Computer Security Incident Response (CSIR)」のためのベスト・ソリューションをご提供する。日米企業への豊富な経験をもとに、CSIR のベスト・プロセスとそのプロセス構築をサポートする。事業分野はセキュリティ・コンプライアンス対応、情報漏えい対応、コンピュータ調査、フォレンジック、訴訟対応に関連する「ソフト販売」「ハードウェア販売」「トレーニング」「コンサルティング」を提供。特に、米国訴訟における電子証拠開示 (eDiscovery) においては、迅速な日本語サポート体制とベストツールの活用により、顧客企業に「コスト」と「対応時間」でもっとも効率のよいソリューションを提供できることを強みとする。 www.ji2.co.jp

1. 最新ビジネス・ニュース

Guidance Software 社と Protiviti 社が戦略的提携し、新しい社内 eDiscovery サービスを提供

10月28日に Guidance Software 社は、世界的なビジネスコンサルティングと内部監査を手掛ける専門ファームである Protiviti 社との戦略的提携を行うと発表しました。

<http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=343408>

このグローバルな提携により、組織が社内で eDiscovery プロセスを管理し、高コストなアウトソーシングを避けることができるよう、テクノロジーとコンサルティングサービスを組み合わせたソリューションを提供するそうです。その提携は、Guidance Software 社の EnCase eDiscovery と Protiviti 社のリスクに対する強力な専門知識とアドバイザリサービスを組み合わせたものです。

この提携では、Protiviti 社は、Guidance Software 社の EnCase eDiscovery ソフトウェアとテクノロジーを Pay-Per-Use (利用分のみ支払う方法) という効率的な形で使用します。これらのサービスを通じて、企業はすぐに Protiviti 社のディスカバリ危機管理チームの利便性を認識することができます。今回の提携により、法的ディスカバリ要求に応えるレベルでの利便性、一貫性、コスト削減、持続性がもたらされます。

日本での展開はまだのようですが、Protiviti も eDiscovery のサービス企業としてトップを模索しているのが読み取れます。

Protiviti 社について : Protiviti 社(www.protiviti.com)は、Robert Half International 社の子会社で、世界中に 60 以上の拠点を持っています。グローバルビジネスコンサルティングおよびリスクアドバイザリ、取引サービスに特化したエキスパートによって構成されている内部監査会社です。Protiviti 社は、専門に特化したファームとして、金融、取引、業務、テクノロジー、訴訟、ガバナンス、リスク、コンプライアンスといった点における問題解決のサポートを行っています。

携帯電話の盗聴について：(メールも含む)

偶然にも携帯電話を盗聴するソフト開発の話が米国で耳にしました。これは、サブレット (エージェント) を強制的に携帯電話に通信経由で流し込み、メールも含め携帯電話の通話を盗聴可能にするものです。対応電話機種は、ブラックベリーなど限られていますが、かなり違法性が強い表舞台に出ることなく南米で開発が進んでいるものです。日本の警察への販売を持ちかけられましたが、市場性がないため?の疑問符がつく製品でした。

ちなみに、米国の法執行機関通信支援法 (Communications Assistance for Law Enforcement Act = CALEA) は、法執行機関が傍受可能な形でネットワークを構成するよう、電話サービス提

供者に義務付けています。 有線、ケーブル・モデム、衛星、無線、電力線などあらゆる方式の
ブロードバンド・インターネット接続サービスを提供しているプロバイダが CALEA の対象となり、
VoIP も CALEA に従い盗聴可能とする米連邦通信委員会 (FCC) の規制案があります。

<http://www.fcc.gov/calea/>

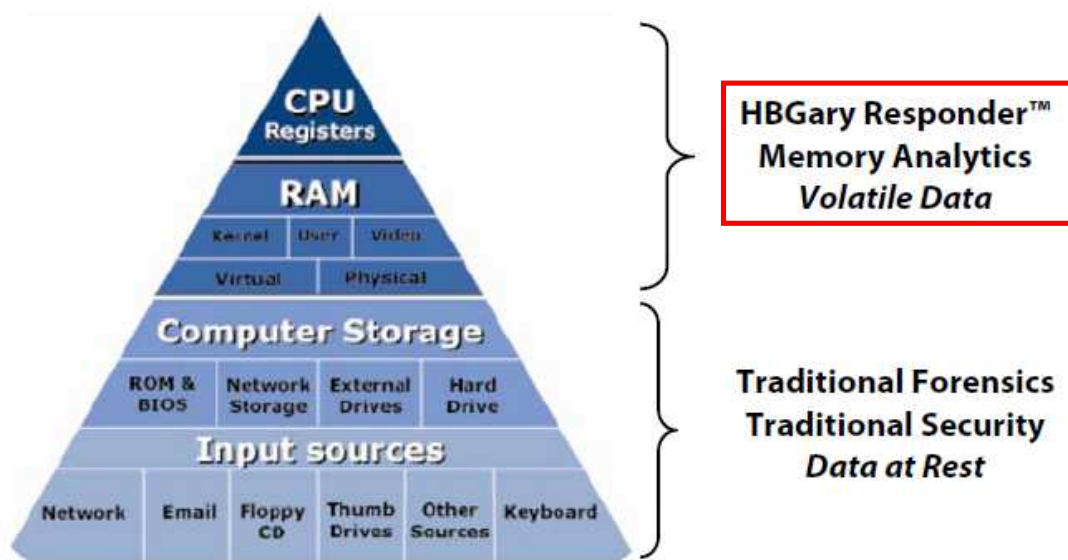
2. テクニカルニュース

メモリーフォレンジックについて：HBGary（メモリ解析ツール）

既存のウィルスソフトウェアは、新種マルウェアの20%程度にしか効果がなく、ゼロデイ・アタックに無防備な企業IT環境であると専門家は訴えています。また、FBIによるとコンピュータ不法侵入とサイバースパイ活動で、毎年1,000億ドル(1兆円)以上の米国での潜在被害を指摘しています。これらの問題に対し、今までのフォレンジック技術ではハードドライブ（HDD）などのストレージ（記憶媒体）の調査にとどまり、調査の不備を指摘されておりました。

そこで近年は、稼働メモリー（RAM：CPU）上のデータの解析を行うことで、解析力を向上させるツールや手法が普及してきています。つまり、メモリ情報を保存、分析できるということは、稼働中のプロセス、開いているファイル、平文のパスワード、暗号化されていないデータ、インスタントメッセージ、インターネットプロトコルデバイス、キーボードモニタ、トロイの木馬やルートキット、開いているポートやリスニング中のデバイス、レジストリ情報、ワイヤレス接続のデバイス、バックされていないバイナリ情報を取得・解析できるということになります。

今回紹介するHBGary Responderは、物理メモリー（RAM/CPU）データを保存し、解析分析するソフトウェアです。HBGary Responderが取り扱う範囲をわかりやすく概念図で示しますと以下のようになります。



HBGary Responderは、大きく分けて2つのフォレンジック機能を有しています。1つ目は、ライブメモリフォレンジックスでルートキット検知などを取り扱います。2つ目は、ランタイムとバイナリのフォレンジックスで、こちらはマルウェア解析、脆弱性攻撃やバグなどを取り扱います。

例えば、マルウェアの調査として、ステルステクニック、レジストリキーとその変更、ロードされたドライバやモジュール、ネットワークソケット情報、ファイルシステムのアクセスと変更、

マルウェアの生存性、暗号キー構成要素、ファイルのパッキングと難読化、コマンドとコントロールメカニズムといった情報が得られます。また、再構築されるオブジェクトテーブルには、割り込みテーブル、全ての分析されたストリングス、全ての分析されたシンボル、全てのオープンファイル、全てのオープンネットワークソケット、全てのオープンレジストリキー、ドライバ、そしてプロセスなどが含まれます。

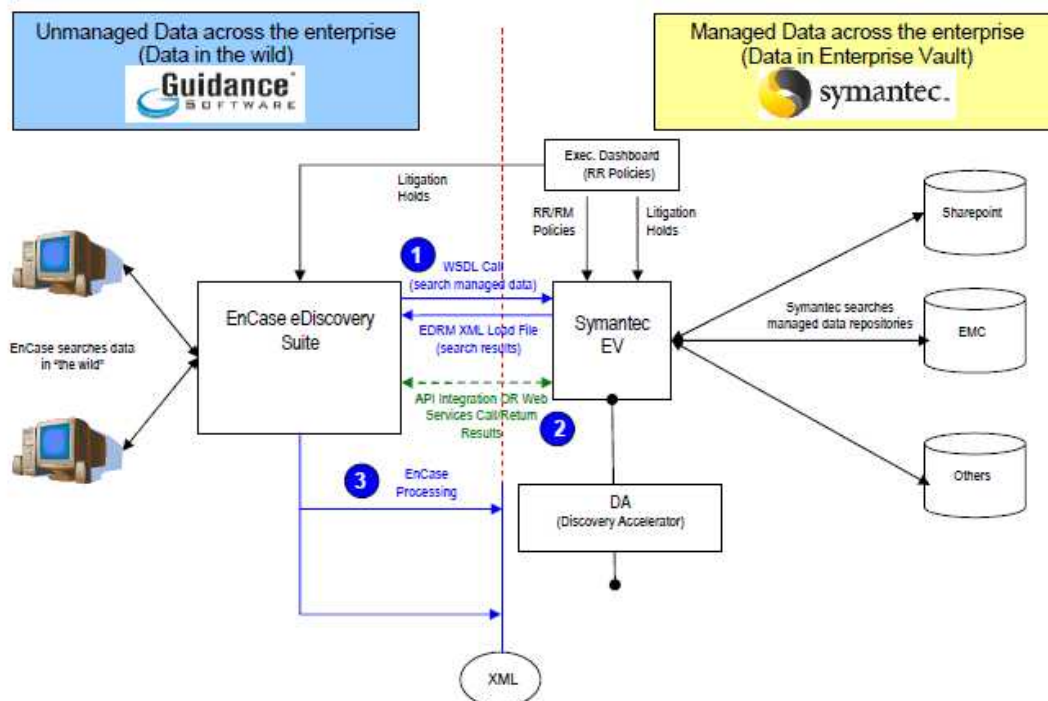
HBGary Responder には EnCase をプラットフォームとしたプラグインが用意されており、EnCase をすでにお持ちのコンピュータフォレンジック調査員は、フォレンジックのルールに基づく手法で Windows コンピュータ上の RAM にアクセスし、RAM の内容を保存、分析、報告することが可能となります。

HBGary <http://www.hbgary.com/products.html>

EnCase eDiscovery モジュールが Symantec 社のメールアーカイブ製品

Enterprise Vault に対応

Symantec 社のメールアーカイブ製品である Symantec Enterprise Vault は電子メールのアーカイブとして世界的に使用されており、社内の電子メール検索に有効な製品です。この度、新たに社内のメール以外のファイル検索で、EnCase とのプラグインが発表される予定です。このプラグインにより、社内電子ファイルの全てを対象にフォレンジックをベースとした検索・取得ができるシステムの構築が可能になります。



3. 製品紹介

Guidance Software 社が EnCase Legal Hold について発表

10月5日に Guidance Software 社は、EnCase Legal Hold について発表しました。
<http://investors.guidancesoftware.com/releasedetail.cfm?ReleaseID=340562>

Legal Hold とは、裁判で対象となりえる証拠などを改ざんすることなく保存することで、裁判手続きの一部です。EnCase Legal Hold は、電子的に格納された情報(ESI)を Web ベースで訴訟ホールドと追跡するソリューションです。

この EnCase との統合的ソリューションは、企業の法務部門が訴訟の初期段階で、法的訴訟ホールド（証拠データの的確な初期保存）のために調査対象端末を識別、通知、更に管理、追跡をし、ESI の実際の保存、収集、処理に関して報告する事を可能にします。

EnCase eDiscovery と EnCase Legal Hold の統合は、EnCase eDiscovery で実行している ESI の収集と処理に関する追跡と報告に加え、調査対象端末への通知や確認を可能にします。

訴訟当事者は、1つのケースにつき1つのデータベースを使って訴訟ホールドを出したり、調査対象端末の確認をしたり、ホールドの順守をモニターしたりする事で、潜在的に関連した ESI の収集と処理の過程もコンプライアンスに沿って行うことが出来るようになります。

Forensic Dossier (ドシェ) について

HDD の容量は日進月歩でますます大容量化しており、その中に納められるデータ量も必然的に多くなってきております。そうした大容量化した HDD を証拠保全する上で利用する機器の処理能力は、証拠保全に係る時間に大きな影響を及ぼすわけですが、今回は処理スピードが世界最速と言われている Logicube 社 <http://www.logicube.com/> の Dossier (ドシェ) をご紹介します。

Logicube 社の Forensic Dossier (ドシェ) は、デジタルフォレンジック調査の様々な問題に対応できるよう設計された、Logicube の第6世代コンピュータ・フォレンジック・ソリューションです。ハイスピード、コンパクトな本製品は、SATA/IDE ハードディスクや様々なフラッシュメディアから素早くデータを取り込むことができます。また、複数の調査対象 HDD からの証拠保全および複数コピー作成（1台または2台の調査対象 HDD から1台または2台の証拠 HDD へ同時コピー）により、解析作業のスピードアップを実現します。これからのフォレンジックの中心的プラットフォームとなる Dossier は直感的で使いやすく、日々進化するハイテク犯罪にも確実に対応することができます。

大きな特徴としては、HDD の種類や容量により異なりますが、現在市場に出回っているものの中では最速であり UDMA6 モードでは 6GB/分のキャプチャスピードを実現しております。2つの独立したクローニングエンジンおよび4つの独立したハッシュエンジン搭載が、この高速処理を可能としております。その実力はキャプチャスピードを落とすことなくリアルタイムで MD5 と SHA-256 を同時計算するときに威力を発揮します。また対応メディアは、SATA/IDE ハードディスクだけでなくフラッシュメディア、RAID のキャプチャにも対応しております。その他、

CloneCardPRO を使いますと HDD の取り外しが難しいノート PC などに接続してデータを取り込むことが可能となり、非常に便利です。

4. アップデート情報

EnCase プロダクトアップデート

EnCase Enterprise バージョン 6.12 (英語版) リリース: EnCaseバージョン6.12がリリースされました。

新機能 :

SHA1ハッシュを証拠ファイルに追加

SHA1ハッシュ計算 EnScriptで、SHA1とMD5を計算、出力できるようになりました。

ロールあたりの接続数設定 SAFE管理者は特定のロール(役割)のための同時接続本数をオプション指定できるようになりました。

スナップショット拡張 ARPテーブルとルーティングテーブルの情報が、スナップショットの一部として取得し、表示できるようになりました。

単語全体検索 単語全体にマッチするものだけを検索する機能が追加されました。

インデックス強化 インデックスケースウィザードでは、包含条件が使えるようになりました。

ProSuiteの64bit対応 ProSuite内のモジュール全て(EDS, VFS, PDE)が64bit版 Vistaに対応しました。これにより、Vistaの32bit版、64bit版の両方がサポート対象となります。

SecureDoc統合 WinMagic社とのパートナーシップ提携によりSecureDoc暗号化ドライブの復号機能が利用できるようになりました。

Utimacoチャレンジ/レスポンス対応 Utimaco暗号化ドライブのデータを見るためにチャレンジ/レスポンスコードを入力できるようになりました。

破損EDBファイルのマウント対応

Neutral status変更 SAFEのネットワークツリー内で「Neutral Status」を設定した場合の意味合いが変更されました。ネットワーク範囲がNeutralとして設定された場合、セキュリティ的な理由からそのネットワークツリー内に明確に含められない限りはこの範囲のマシンはアクセスできないようになりました。

5. イベント情報

日本国内

・シマンテック/Ji2 eDiscoveryコンサルティング協業の記者発表会

日時: 2008年12月8日

場所: シマンテック本社 (赤坂)

・第5回デジタル・フォレンジック・コミュニティ2008 in Tokyo

日時: 2008年12月15日～12月16日

場所: ホテル グランドヒル市ヶ谷

<http://www.digitalforensic.jp/index.html>

このニュースレターは、お申し込みをいただいた方へ配信しております。
ニュースレターの登録、解除等については、下記アドレスまでご連絡ください。
本ニュースレターに関するご要望、ご意見をお待ちしております！

編集・発行

株式会社 Ji2 (発行担当: 佐藤)

E-mail: newsletter@ji2.co.jp

11235 Knott Ave. Suite C. Cypress, CA 90630 U.S.A.

〒160-0004 東京都新宿区四谷4丁目3番地802号

TEL: 03-6228-0163 FAX: 03-6228-0164 <http://www.ji2.co.jp/>
