

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10月号

2008年も既に秋に入り徐々に紅葉も進んでおります。我がJi2も米国経済の最近の大きな変化とともに、色とりどりの秋がやってきたと感じております。

弊社Ji2は、2001年より米国で、そして2008年2月より日本法人を開設し、本格的に「フォレンジック」・「インシデントレスポンス」・「eDiscovery」の業務をスタートさせました。現時点では数少ない「日・米」どちらもサポートできる業者として、ベストプラクティスを求める優良企業にサービスを展開しております。

今後は、本Ji2ニュースレターにて「フォレンジック」・「インシデントレスポンス」・「eDiscovery」の各ビジネス分野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つの分野で発信してまいります。内容につきましては、ご意見・ご希望・ご批判ありましたらご一報いただければ幸いです。

1. 最新ビジネスのニュース < 児童ポルノの取締技術 >	2
2. テクニカルニュース	4
3. 製品紹介 (ZyLABの話)	5
4. アップデート情報	6
5. イベント情報	8

< 今後のカバーするトピック・キーワード : 法律技術 (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 >

1. 最新ビジネスのニュース < 児童ポルノの取締技術 >

児童ポルノに関する米国捜査当局の最近の動き

最近、Limewire などに代表される P2P などで児童ポルノなどを交換している人を観察して捕まえる動きが米国では盛んです。サイバースペースに隠れて行われている自動ポルノに関する行為を、ICE や FBI は常に監視し、そのような活動をしている WEB 使用者を Track しており、すでに 55 名が米国で逮捕されています。(US-ICE の 8 月 19 日付のニュースより)

<http://www.ice.gov/pi/nr/0808/080819losangeles1.htm>

今後、さらに児童ポルノに対する取り締まりを強化できるように「Protect Out Children Act」という法案が米国では上院に提出され可決されています。

<http://itpro.nikkeibp.co.jp/article/NEWS/20080929/315558/>

ここでのポイントは、公共性と匿名性の強いインターネット上の行為が、警察などの観察・調査される対象となるということです。つまり、われわれ個人が卑猥なサイトなどへ接続した場合、IP アドレスが ISP などを介して調査され個人情報付きでブラックリスト入りするというものです。今回の 55 名の逮捕者は氷山の一角で、つまり見せしめです。日本でも今後はこのような抑止効果が、検討される日も近いと考えます？！

動画検索の最新ツール (児童ポルノなどの検索)

児童ポルノや暴力の画像調査では写真やビデオなどの長時間レビューが必要とされます。これは調査官の職場環境を著しく低下させ、レビューによる不快な時間が多くなります。この作業を最小にするため近年は画像マッチの表示やパターン認識による短時間で効率的な画像抽出機能はかなり進化してきました。特に、強力な画像・動画の検索に特化したツールとして LTU-Finder というソフトウェアがあります。このツールの米国 FBI などでの使用はかなり進んでいる様子です。(ガイダンス社 EnCase とのプラグインも可能)

日本でも今後、画像に関するレビューはこのようなツールを使用した効率化が進むと予想されます。

LTU-Finder

<http://www.ltutech.com/en/technology-and-products.finder.html>

ウラ話

米国ロサンゼルスでは知る人ぞ知る、治外法権を利用した米国発の日本向けポルノサイトが運営されているそうです。(サーバーなどは、また別の国にあるのですが、、、)これらの画像は米国では合法ですが、日本では違法というものを取り扱っていると考えられます。だいぶ前に日本の警察の方から、日本と米国でのポルノ画像の違法性見解の違いでお話を聞いたことがあります。

ますが、まさに その狭間をうまく利用してビジネス化しているのでしょうか？いずれにしても、ネット犯罪対策の国際的共同化を推進して、今後は取り締まりの強化をお願いしたいものです。

2. テクニカルニュース

メモリ解析ツール

近年はPCの物理メモリをランタイム中にフォレンジック解析しない限り入手できないデータが増えてきています。具体的には暗号化のキー(BitLockerなど)、P2Pプログラムのユーザ名やパスワード(Skypeなど)、Webブラウザでのサイト訪問履歴(IE8 Privateモード)、ルートキットなどの悪意のあるプログラムなど、これらはHDD上をフォレンジックしても何も形跡を見つけれないケースが多くなってきております。

現時点で、代表的なメモリ解析ツールはHBgary, KntTools, Nigilent32, DD, Volatilityなどがありますが、実際のメモリダンプからの解析は、これらのツールを使用してもプログラムをよく分からない素人(自分)にはかなりハードルの高いものです。また、PCのランタイム中にメモリのダンプを取らなければいけないのは、フォレンジック調査で不可能に近いのではないのでしょうか？(たまたま調査PCがONになっているのを祈るのみ?!)

そこで最近知りえた情報なのですが、アンチウイルス会社はメモリ解析を現在でもMalwareに対して行っており、今後はメモリ解析ツールを同じエージェントに入れて、メモリダンプの解析結果をITの管理者に報告しようという動きになっています。これは既にウイルスメーカーのエージェントが各PCに埋め込まれておりメモリに対してアクセスしていることを利用するもので、2009年度中には製品化されるようです。これで企業でのランタイム中のPCのメモリダンプは取り放題になるわけですが、引き続き問題は「解析の簡易化」です。

EnCase 関連

HELIX 2.0 リリース

EnCase Ver5までは、EnCase 起動ディスクはFDかCD-ROMで起動するMS-DOSベースのものでしたが、EnCase Ver6からはLinuxベースで起動するLinEnが提供されています。

ガイダンスソフトウェア社(以降GSI)が提供しているKNOPPIXベースの起動ディスク(1CD-LINUX)でLinEnを利用することもできますが、従来からHELIXにはLinEnが含まれていました。(GSIのサポートページではHELIX 1.9aのISOイメージも提供していますね)

さて、9月15日には待望のHELIX 2.0がリリースされました、従来KNOPPIXベースであったHELIXですが、UbuntuベースとなりUSB接続されたCD-ROMドライブからの起動にも対応しています。HELIX 2.0には、LinEn最新版の6.11.2と共に、Windows用のメモリダンプツールである、WinEnも含まれるようになりました。

余談になりますが、HELIXのWebページには大きくHELIXの横に「3」という文字があるため、一瞬HELIX 3.0と勘違いしてしまいそうですが、「3」の意味は三つのミッション”インシデント・レスポンス、コンピュータフォレンジック、Eディスクバリ”を示しているそうです。

HELIX <http://www.e-fense.com/helix/>

3. 製品紹介 (ZyLAB の話)

コンピュータ・セキュリティにおいて、インシデントリスポンス作業の大きなチャレンジは、必要なデータの場所を的確に把握して、迅速に必要なデータを抽出することです。例えば、図書館で本が位置管理されることなく無造作に読み置かれている状態を想像してください。ここでは、いかに読みたい本を探すのに苦労するかが分かります。現在、企業の電子データは、その図書館状態であり体系的に管理されていない状態にあります。そして、この図書館の本の整理を行うのがRM(レコードマネージメント)ツールです。

今後は、フォレンジック・インシデントリスポンス・eDiscoveryなどの分野とRMは密接な関係を持つてくることは間違いなく、今回はRM製品として実績のあるZyLabを紹介いたします。(eDiscoveryなどのツールとして米国で導入企業実績が多い製品です。)

ZyLAB テクノロジー社について

ZyLAB テクノロジー社はデジタルアーカイブアプリケーションを開発している、世界的に有名な会社です。その始まりは1983年シカゴで、現在は本社をバージニア州とアムステルダムにおき、積極的な世界展開を進めています。

その製品は主に、ZyIMAGEとZyINDEXという二つの主力製品から成り、いかに必要な情報を必要なときにすばやく取り出すことができるか、という点を主眼に、社内データベースやOCR読み込み情報などの整理、管理を行うソフトウェアとなっています。古くはDOSバージョンのIBM PCのテキストデータを管理するソフトウェア製品の提供から始まり、現在ではガートナーのマジッククワドラント、“インフォメーションアクセステクノロジー”部門のリーダーとして位置づけされている老舗です。

ZyIMAGE Information Access Platform (IAP)

ZyIMAGE Information Access Platform(以下、IAP)について簡単にご説明いたしますと、IAPは完全なXMLベースのシステムです。デジタル化された紙文書から、電子ファイル、Eメールや添付ファイル、マルチメディアにすべての不可欠な情報をアーカイブし、それらを長期管理するための基盤を提供します。

そして、その基盤を提供する基となっていますIAPコアテクノロジーは、標準的なブラウザを通して速くて、簡単で、安全なやり方をとりながら、特定のデータを見つけ、アクセスして、纏めることができるのが特長であります。また、ユーザは、彼らが特定のプロジェクトまたはビジネスプロセス(レコードマネージメント、ワークフロー、eDiscoveryとeDisclosure、その他もろもろを含む)の間に必要とする正確な、費用効果がよいソリューションをつくるために、さらなるモジュールを追加することができます。

ZyLAB <http://www.zylab.com/index.html>

4. アップデート情報

EnCase プロダクト アップデート

EnCase Forensic バージョン 6.11.2(英語版)リリース: EnCaseバージョン6.11.2がリリースされました。

新機能:

LEF EFS暗号化強化

WinEN WinENは、稼働中のWindows(2000以降)の物理メモリを取得するためのコマンドラインユーティリティです。

DBモジュールセットに対するスナップショット ネットワーク越しにノードのスナップショットを取得し、SQLデータベースに格納します。また、スナップショットに関するレポート作成のために、そのDBから読みこみをします。そのDBに対して最小限のメンテナンスを許可し、格納されているデータ量をコントロールすることができます。

Lotus NoteローカルDB暗号化 ローカルのLotus Noteユーザーメールボックス(NSF file suffix)に対応しました。

ExaminerのMicrosoft Vista対応

64bit EnCaseサブレット対応 対象はWindows XP, 2003, およびVistaです。

HBGary Responder用Encrypt メモリ情報をHBGary Responderに渡します。

EnCase Enterprise / FIM バージョン 6.10 リリース: EnCase Enterprise バージョン6.10 がリリースされました。

新機能:

メモリアクセス コンピューター内のRAMと各プロセスのメモリスペースを視覚的に見ることが可能です。ロール付加機能付でリードメモリの有効無効の設定機能もつきました。

LVM, LVM2 サポート

ソラリス10(ZFSつき)ファイルシステム対応 32bitと64bitカーネル両対応です。

Credant サポート Credantの暗号化ファイルに対応しました。

Safeboot サポート Safebootバージョン4 と5 に対応しました。

64bit Utimacoサポート 64Bitのエグザミナー用にUtimaco SafeGuard Easy のバージョン4.50.0.1 以上に対応しました。

S/MIME ファンクション 暗号化MBOX, EDB, PSTフォーマットS/MIME暗号化Eメール(RSA標準PKCS7対応)の機能を備えました。

VISTAサムネール Windows VISTAの新しいサムネールキャッシュに対応しました。

インターネットブラウザ対応機能強化

フィルターカラム機能強化

プライムクラスタGDS ソラリス8,9,10 の32bit と64bit サーマレットがアップデートされ、プレビューやスナップショット、ライブプライムクラスタのボリュームからのデータ抽出に対応しました。

5. イベント情報

日本国内

- ・EnCase Computer Forensics I トレーニングコース

日時: 2008年11月 11日 ~ 11月14日

場所: 情報セキュリティ大学院大学

http://www.ji2.co.jp/software/encase/training_detail/index2.html

- ・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>

EnCase Forensic トレーニングの近況

米国ガイダンスソフトウェア社公認「EnCase Forensic トレーニング」の内容が最近変わったことをご存知ですか。従来、EnCase Forensic 初級(エッセンシャル)、中級(インターミディエイト)と呼ばれていたコースは名称が変更され、Computer Forensic I というコースになりました。

Computer Forensic I (以後 CF1) コースでは、EnCase の基本的なケース管理方法から始まり、ファイルの種類を自動的に識別するシグネチャアナライズ、ハッシュアナライズや検索機能などについて学ぶことができます。CF1 を受講した調査官は、Computer Forensic II (CF2) トレーニングに進むことで、より高度な GREP による検索方法や、Windows コンピュータ上に存在するアーチファクト(artifact)について学ぶことができます。Windows 上には様々な調査上の手がかりが存在していますが、どのようなデータが何処に、どの様に保存されているかを CF2 コースでは扱います。

CF1・CF2 いずれのコースも、コース専用開発されたシナリオと証拠ファイルを使い、実際のデジタルデータを調査しながらトレーニングを受けることができます。また、今後開催されるコースは、日本人講師による日本語でトレーニングを受講いただけます(ソフトウェア・証拠ファイルなどは英語になります)

また、CF1 コースが 11 月 11 日 ~ 14 日に開催予定です。EnCase の本格的なトレーニング受講をご希望の方、CF2 コースの受講をお考えの方はぜひ CF1 から受講をお願いいたします。

Ji2 では、日本の EnCase ユーザ様に、より充実したトレーニングの提供を目指して頑張っておりますので、今後も Ji2 の EnCase トレーニングにご注目ください。

EnCase トレーニングに関する詳細

<http://www.ji2.co.jp/software/encase/training.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います！

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/>
