

## Ji2 ニュースレター (フォレンジック・インシデント・レスポンス専門情報)

2007年11月号

1. フォレンジック業界の未来図 .....	2
2. Symantec が Vontu を買収する意味 .....	4
3. インシデント・レスポンス関連 HOT トピック .....	6
4. Security Solution 2007 に参加して (東京ビッグサイト) .....	8
5. 製品アップデート情報 .....	9
6. イベント情報 .....	11

## 1. フォレンジック業界の未来図

---

情報セキュリティ分野でフォレンジック業界のニッチ性を利用して、米国ではガイダンスソフト社が前年度に上場し、日本ではUBIC が今年上場を果たしました。ガイダンス社 (2007 年度・売り上げ予想 : 80 億円?) は EnCase ソフトというソフトウェアを中心とし、UBIC (2007 年度・売り上げ予想 : 6 億円?) はコンサルサービス中心のビジネスですが、どちらも 2007 年度のフォレンジック業界の幕開けを十分に情報セキュリティ業界に示したと思います。

それでは、これからの 2008 年度の業界はどうなるのでしょうか? フォレンジック業界の収入源はフォレンジックソフト・コンサルサービス・トレーニングの 3 つがメインなのでこの分野での今後の動きを Watch しました。

### 1. フォレンジックソフト

FTK いよいよ最新の 2.0 版を出荷予定です。新機能は下記リンクでアナウンスされていますが、「日本語コードページ検索機能」の追加と、「携帯電話データ取得機能」(日本の携帯は残念ながら発売開始時にはサポートしないようです) が既存機能の強化とともに使いやすくなりそうです。

\*弊社 Ji2 も FTK のユーザなので、来週開催される、お披露目会に参加予定ですので、詳細は後日報告します。

<http://www.accessdata.com/common/pagedetail.aspx?PageCode=ftk2test>

\*\*裏話としては、FTK のメーカーである Access Data 社に、ガイダンス社の元社員がかなり入社しております。ガイダンス社のフォレンジック業界で 1 強時代を崩すべく、単独フォレンジック版(ネットワーク版でないもの) は面白い時代になりそうです。

**携帯フォレンジック・ソフト**は今米国では花盛りです。ガイダンス社のニュートリノ <http://www.encase.com/products/neutrino.aspx> という製品は発売から 1 年以下で世界中で 1,000 台近く出荷しました。(3 億円くらいの売り上げです!)

ただし、日本携帯のサポートになると、現時点での最有力は米国サステーン社の Data Pilot という製品です。サステーン社は日本の携帯バックアップソフトなどにもエンジン供給している会社で、日本 + 世界の携帯電話対応で一気に 900 モデルのサポートも可能です。

<http://www.susteen.com/productdetail/253/producthl/Notempty>

( 来年 1Q で日本語携帯サポート版の発売予定ですので、詳細は Ji2 にお問い合わせください。 )

## 2. コンサルティング・サービス

米国では E-Discovery 法とも呼ばれる Federal Rules for Civil Procedure (FRCP) が前年度の 12 月に施行されました。このため電子証拠取得を日本の大企業も日本国内で余儀なくされており、今後は UBIC などが行う裁判対応のフォレンジックサービスが増加すると考えられます。ただし、日本での法整備が米国より遅れているため、今後の日本での業界成長はゆっくりとしているのではないのでしょうか？そして米国の状況から推察すると、UBIC がこの分野での独占企業となることは難しいような気がします…。

( 成長が著しいときに、多くの企業が参入！？ )

## 3. まとめ

注目しなくてはいけないのは、むしろ E-Discovery のソフト分野で、EMC 社や Symantec 社などが、企業のデータベース検索ソフト ( E-Discovery 技術 ) の開発に躍起であることでしょう。特に、検索技術を持つ会社のここ数年で大きな買収の動きが進んでいるのが不気味です。大手アンチウィルスソフトメーカー、マカフィー は 2006 年にオニグマを現金 2000 万ドルで買収し、同年おなじくセキュリティソフトウェアメーカーの ウェブセンス がポートオーソリティを現金 9000 万ドルで買収しました。将来はガイダンス社が、Symantec 社に買収される？！などの再編も、E-Discovery 関連のソフトが成長することで考えられます。ここで私たちは、日本語の検索技術に卓越した企業が日本市場では必要であり、この観点で今後のビジネスの布石を打つ必要があると考えます。

## 2. Symantec が Vontu を買収する意味

---

2007 年度 12 月までには、VONTU 社が Symantec 社に買収されることが正式に決定致しました。日本でのビジネス展開において VONTU 社とパートナー提携している Ji2 にも、正式に以下のような連絡がありました。

「今日はお伝えしたい重要なニュースがあります。今日、私達は、VONTU が正式にシマンテック社の一部となる書類にサインをしたことを発表します。私達はこの機会を世界的なクラスのソフトウェア会社となり、私達のビジネスを拡大する良い機会として非常に期待しています。

私達は引き続きシマンテック・データ・ロス・プリベンション(DLP)チームとしてお客様への今までと変わらぬサポートを致す所存です。チームは今まで通りの開発、製品管理、販売、マーケティング、プロフェッショナルサービスとサポート部門を引き継いでいます。

製品に関しましては、シマンテック社の製品と融合した、エンドポイント・プロテクション、ネットワーク、ストレージ、コンプライアンスソリューションといった更なるリソースを追加してより一層の機能拡張を図ります。シマンテック社と VONTU 社の技術を合わせてより強力な DLP を提供できる立場となります。また同時に、スタンドアロン製品として今まで同様の VONTU 製品を提供し続けるつもりです。

私達 VONTU に寄せて頂いている信頼と確信に感謝しております。私達はできる限りスムーズな移行と成功を見据えた充実した関係を築くよう、引き続き協力を続けていきたいと願っております。いつも惜しめない援助に心から感謝致します。 - ジョセフ・アンサニール、CEO/チェアマン - VONTU, Inc.」

シマンテック社の発表によると、買収金額は 3 億 5000 万ドルの全額現金で行なわれ、第 4 四半期中に完了する見込みとなっています。買収の目的は、シマンテック社の次世代セキュリティ構想「Security 2.0」に必要となるエンドポイントおよびネットワークセキュリティ、ストレージとコンプライアンスに関連する既存の製品群を補強することで、VONTU のデータ監視および漏洩防止ソフトウェアは、機密データが E メールやインターネット、インスタントメッセージングで社外に流出することを防ぐほか、リムーバブルメディアへのコピー

やローカルドライブへのダウンロードも防止し、ポリシー管理およびデータ漏洩の検出、データ復旧処理をすべて一元管理できるプラットフォームを提供します。

Vontu は Symantec の情報漏えいの独立専門部門としてスタートし、始めは Symantec 製品へ Endpoint や E-Discovery 用へ検索エンジンを供給します。Vontu 製品に関する、製品や人員の変更も無く、製品の導入・運用でご迷惑かけることは無いと考えております。

VONTU の高い技術がシマンテック社の一部となることにより、業界トップの位置をさらに高め、独走体制を築いていく第一歩となるに違いありません。Vontu は Symantec の独立 DLP(情報漏えい) 部門として、Ji2 も日本での契約続行で DLP 専門業者として引き続き協力します。

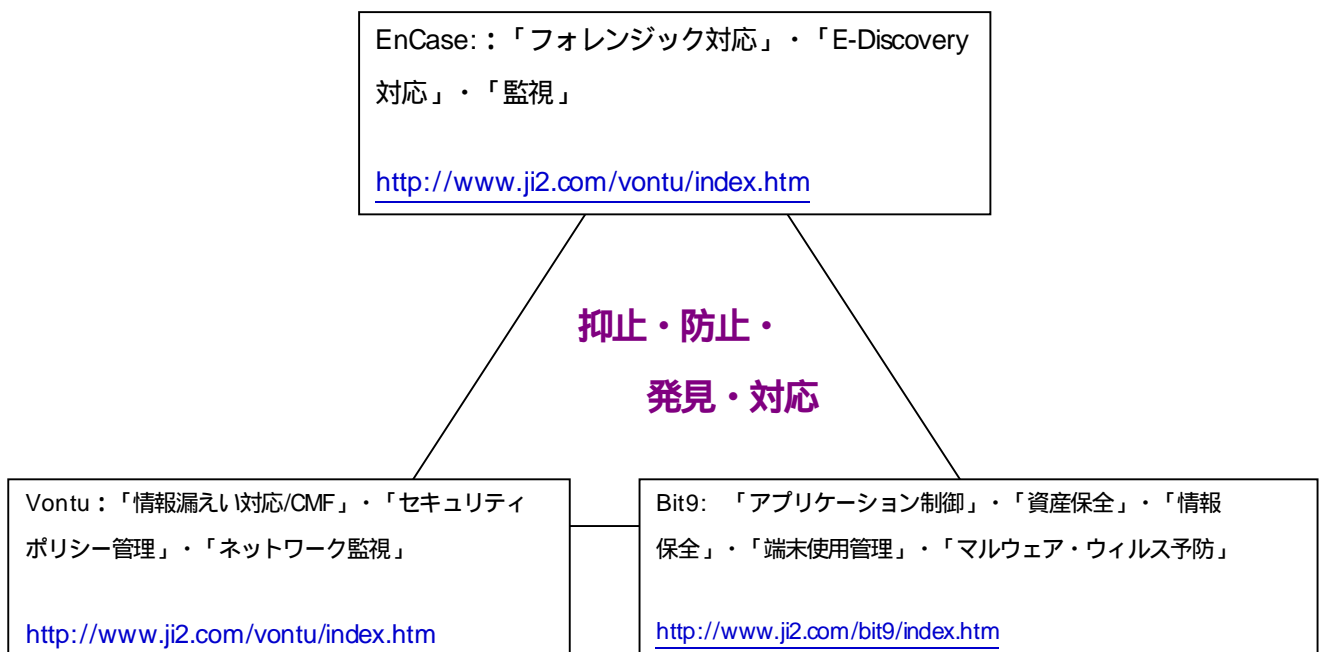
### 3. インシデント・レスポンス関連 HOT トピック

#### ソーシャル・メディアのインシデント・レスポンス

最近ではブログ、Wiki、SNS（ソーシャル・ネットワーキング・サービス）、ビデオ共有サービスなどのソーシャル・メディアを社内で使うケースがあります。米国でいうと「MySpace.com」や「iTunes」「Flickr」「YouTube」といった、Web 2.0の世界に到達します。これらのセキュリティ対策は、「ウイルス対策ソフト」、「ネットワーク監視」、「URL フィルタリング」、「アプリケーション制御」、「Web 評価サービス」および「セーフ検索」ツールを組み合わせた統合的な対応が行われているが、最近では、これにCMF（コンテンツ監視/フィルタリング）と呼ばれる分野のツールをよく使います。（弊社 Ji2 取り扱い製品で言えば Vontu）CMF を使えば、危険な Web サイトへのアクセス・ブロックのほか、データ・ストリームからあらかじめセットした文字列を検索して、従業員が社内の PC からどんな投稿を書いているかまで監視できるのが特徴で近年米国では導入が盛んです。

#### 注目のセキュリティ製品統合化対応製品

弊社 Ji2 はセキュリティ統合化対応の「抑止・防止・発見・対応」の4つのフェースで世界 No. 1（シェアトップ）の日本語化製品を下記のように紹介しております。



## **携帯電話のフォレンジック製品**

弊社 Ji2 では、日本携帯電話専用フォレンジック対応ハードウェアとソフトウェアについて実績ある既存有名メーカーと協力し実用化を進めています。今後の提供と情報のアップデートにつきましては随時このニュースレターでお知らせ致します。プロトタイプの実施を製品 R&D のため無料でさせていただいておりますので、皆様からのリクエストもお待ちしております。

## 4. Security Solution 2007 に参加して （東京ビッグサイト）

---

先の 10 月 24 日から 26 日にかけて、東京ビッグサイト東展示ホールにおいて、Security Solution 2007 <http://itpro.nikkeibp.co.jp/ev/secu-ex07/index.html> が開催されました。東芝ソリューションや日立、富士通といった大手メーカーをはじめ約 120 もの企業がブースを連ね、最新のセキュリティ製品、ソリューションの情報を提供し、のべ 27886 名の方々がご来場されました。

今年の特徴は、非常に多くのブースで“DLP”（Data Leak Prevention）の文字が掲げてあったことです。日本語で簡単に言えば「情報漏洩対策」製品ということなのですが、米国のセキュリティ製品の動向に合わせて DLP という表現が大きく使われていました。米国製品も徐々に入ってきており、また日本製のものも含めて、統合製品という形で DLP 製品が数多く紹介されていました。その中には日本独自のログ収集やデバイスコントロール（外部機器へのデータ移動の管理制御）の製品も沢山ありました。

世界が注目している DLP のソリューションは「コンテンツモニター：CMF」と呼ばれる最新セキュリティ技術です。性能や程度の違いはありますが、ポリシーにしたがってデータの中身を判別して情報漏洩を止めたり、ネットワーク上のデータを監視することができます。（米国製品の Websense、マカフィー、CodeGreen、LeakProof、Vontu などが CMF 製品関連では今回出展していました。）

新たな技術も含め、米国同様日本でも徐々に情報セキュリティ製品の流れが DLP の方向へ向かっているということを肌で確認することができました。

私達 Ji2 も DLP 製品で CMF 技術米国最大手「VONTU」、そして、アプリケーションコントロールの「Bit9」、フォレンジック分野で「EnCase」といった製品を紹介させていただきました。

ご来場頂いた皆様、どうもありがとうございました。

## 5. 製品アップデート情報

---

### EnCase プロダクト アップデート

**IA (Information Assurance) :** リリース予定 8月24日

**AIRS :** バージョン2.2 リリース予定。 ペリセプトとVONTUとの完全融合(共用)可能。

**EnCase Forensic(EF) ,Enterprise (EE) , FIM**

EnCaseバージョン6.7.1がリリースされました。

**新機能 :** NSF暗号化サポート、MSG拡張機能サポート、XMLフォーマットファイルのエクスポートツリーとテーブル機能、ガーディアンエッジ対応、レコード内のファイアフォックスキャッシュ、レコードタブ拡張、コードページ対応拡張

**Neutrino :** バージョン1.3リリース。 - Nokia新型携帯電話に対応。 Samsungの問題点を解消。

### **現在の各製品のリリースバージョン**

EnCase 製品	バージョン	リリース日
EnCase Enterprise	6.7.1	8/22/07
EnCase Field Intelligence Model	6.7.1	8/22/07
EnCase Forensic	6.7.1	8/22/07
EnCase eDiscovery Suite	2.1	8/22/07
EnCase Information Assurance Suite	2.2	8/22/07
EnCase Automated Incident Response Suite	2.2	8/22/07
Neutrino	1.3	8/22/07

### VONTU プロダクト アップデート

VONTUバージョン8がリリース予定です。保存された機密データの検出機能、USBデバイスやCD/DVDにコピーされたデータの監視、ウェブメールやIMなどで送られたデータに対応強化しました。

[http://www.vontu.com/news/releases/592\\_release.asp](http://www.vontu.com/news/releases/592_release.asp)

**Bit9 プロダクト アップデート**

Bit9 パリティ バージョン4.0が発表されました。デバイスコントロールでのカテゴリ分け分類表示項目などが追加されました。

<http://www.bit9.com/products/parity.php>

## 6. イベント情報

---

- ・ **第4回 デジタル・フォレンジック・コミュニティ2007**

日時： 2007年12月 17日、18日

場所： ホテル グランドヒル市ヶ谷（東京都新宿区市ヶ谷）

<http://www.digitalforensic.jp>

今年は「リーガルテクノロジーを見据えたフォレンジック」をテーマに、国内外の実務運用等についての講演や研究会、技術説明等で認識を深めるものとなる予定です。

- ・ **ITPro Expo 2008**

日時： 2008年1月 31日～2月1日

場所： 東京ビッグサイト

<http://itpro.nikkeibp.co.jp/expo/index.shtml>

ITpro EXPOは、月間1500万PV（ページビュー）/250万UB（ユニークブラウザ数）を誇るWebサイト「ITpro」から生まれた先進的なイベントです。日経BP社のICT系専門媒体と完全連動することにより、従来の展示会の概念を超えた世界初のクロスメディア型イベントを創り上げます。

- ・ **ICDF2008**

名称： Fourth International Conference on Digital Forensics (ICDF2008)

日時： 2008年1月27-30日

場所： 京都大学

URL： <http://www.cis.utulsa.edu/ifip119/Conferences/>

- ・ **RSA カンファレンス 2008**

日時： 2008年4月23日、24日

場所： ザ・プリンスパークタワー東京

URL： <http://www.cmpotech.jp/rsaconference/exhibitor08/index.html>

RSA® Conference Japan では、暗号、認証、ネットワークへの脅威など、最先端の技術から、情報セキュリティに関する最新の法制度や、企業のセキュリティ対策まで、幅広いトピックを取り上げます。

- ・ **Information Assurance 秋季シンポジウム**

日時： 2007年11月29日

場所： Bethesda, MD (米国)

- ・ **Legal Tech 2008**

日時： 2008年2月5日～7日

場所： ニューヨーク (米国)

---

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：Jin Watanuki）

E-mail: [jwatanuki@ji2.com](mailto:jwatanuki@ji2.com)

11235 Knott Ave. Suite C. Cypress, CA 90630

Warland Business Park U.S.A.

〒102-0081 東京都千代田区四番町 4 番 13 号 井上ビル 4 F

TEL: 03-5212-3190 FAX: 03-5212-3195 <http://www.ji2.com/>

---