



The Leader in Computer Forensics and Incident Response Solutions

# フォレンジックは捜査技術から不正抑止 およびeディスカバリーの中核技術へ

From the Lab to the Boardroom;  
Forensics goes mainstream...

**ブライアン・デュゲイ(Brian Dugay)**  
**CISSP, Security Engineer**  
ガイダンス・ソフトウェア



## フォレンジックとは？

電子記憶媒体上で、あるいはそこから取得されたデータを科学的に精査・分析する技術。フォレンジック的に正しく取り扱われた電子情報は法廷での証拠能力を有する。

フォレンジックの機能が迅速、高度かつコスト効率がよいため、  
すべての組織・企業において、フォレンジックは  
火急のソリューションとして急速に普及……

Intellectual Property Theft

Law Suits

Identity Theft

Malicious Mobile Code

Financial Manipulation

Crime

Regulatory Compliance and Auditing

Corporate Espionage

Political Embarrassment

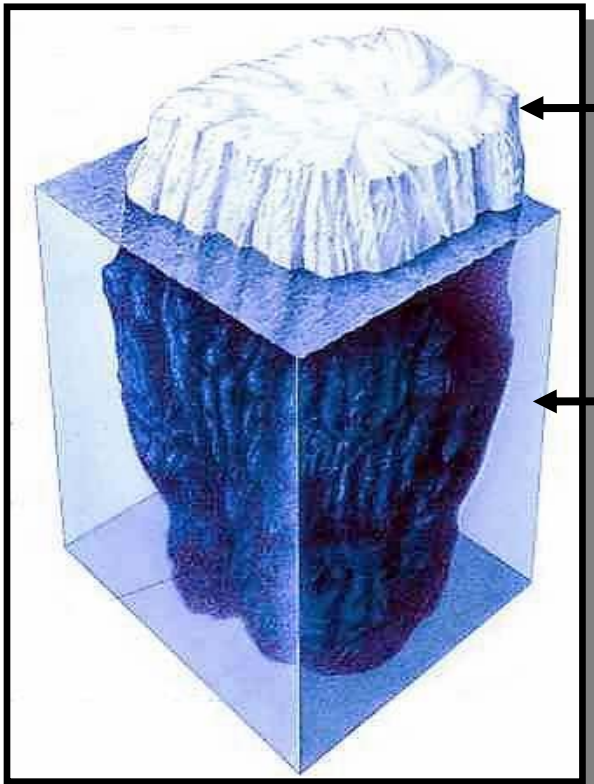
Defacement

Virus Outbreak/Containment

Misuse of Corporate Assets

Mergers and Acquisitions

# Your Data "Iceberg"

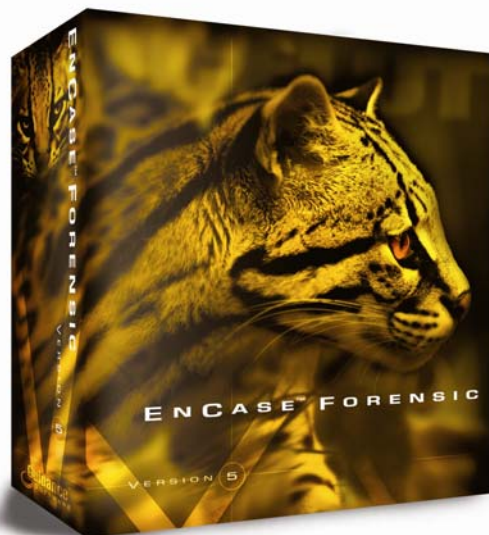


通常のツールで見える範囲は限られている

フォレンジックでは、削除データ、改変データ、  
隠匿データ、埋没データを容易に発見できる

## 世界初のWindowsベースのフォレンジック・ツール **法的証拠能力**

- ① コンピュータの専門知識が不要
- ② 簡単な操作、強力な分析力
- ③ 電子メールとインターネット解析機能

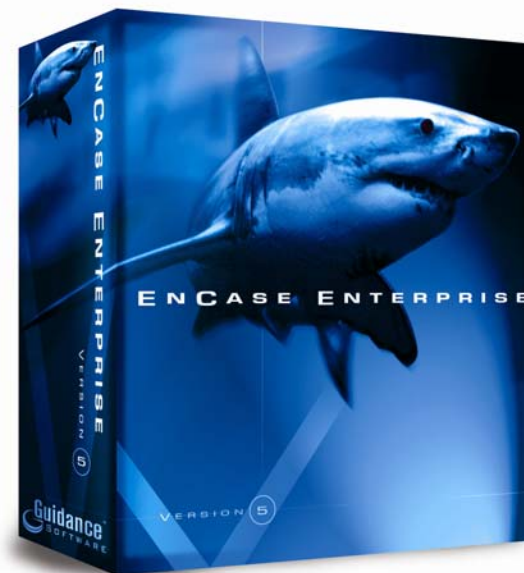


**EnCase Forensic (EF)**

各種法執行機関向け**コンピュータ・フォレンジックの標準品**

**高速・高機能性**により、複雑な調査を正確かつ効率的に行う

- 唯一のネットワーク型調査ソフト
- 米国民事企業訴訟でのデファクト・スタンダード
- 業務を停止させることなく、クライアント側は受動的なままにe-Discoveryが可能
- コンピュータの揮発性データの取得が可能
- ハードディスクの内容をビットストリームデータとして取得(複製)・保存するためのE01形式という専用フォーマットを利用。E01形式でファイルを作成した場合、CRC値とMD5ハッシュ値を自動的に確認する仕組みにより、以降ファイルの内容を変更することはできない

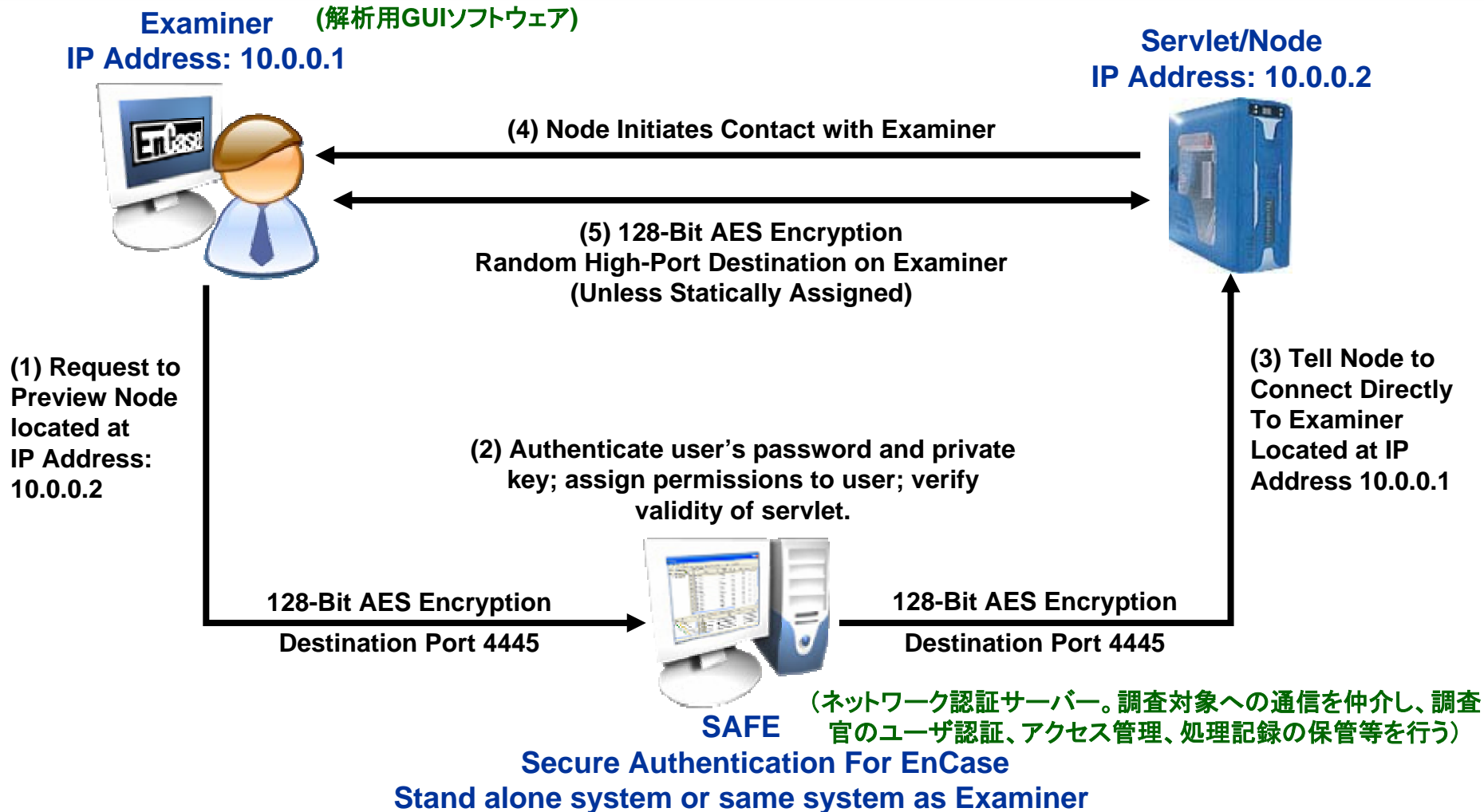


## EnCase Enterprise (EE)

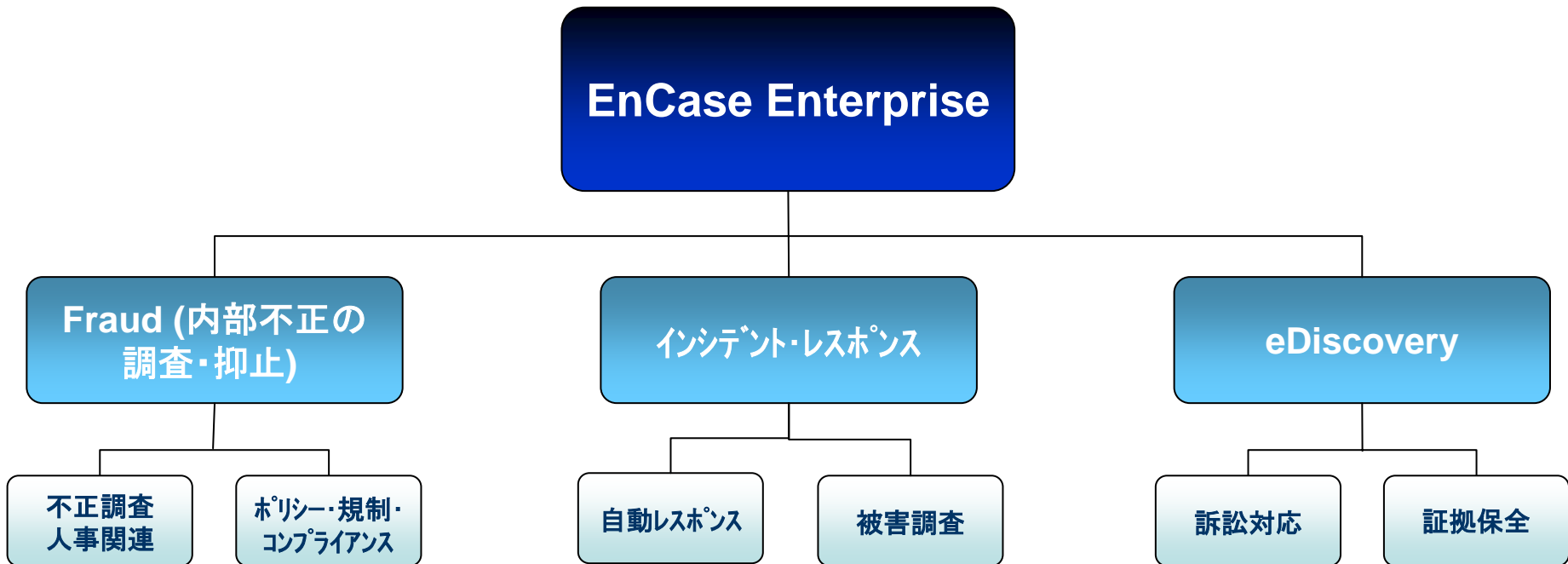
### 充実した解析機能

ハッシュ解析、シグネチャ解析、キーワード解析、ファイルタイプ解析、画像解析、時系列解析  
メタファイル解析、ネットワーク解析、揮発性データ解析、Webサイト解析、メール解析  
メール添付ファイル解析、消去データや未使用領域解析

# EnCase Enterpriseの構成

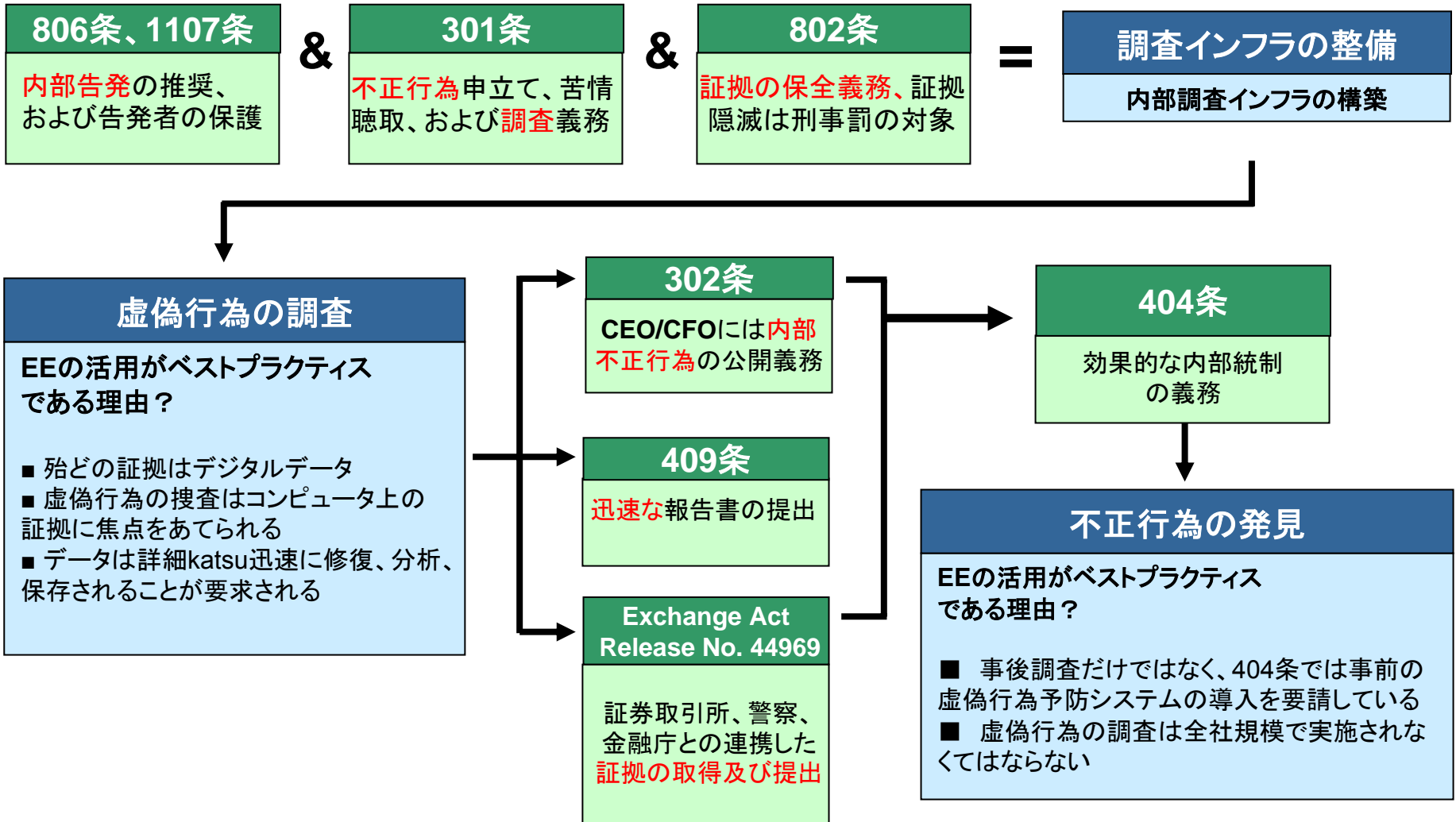


“組織の内部調査およびインシデントレスポンスに、正確、迅速、且つ大幅なコスト削減を実現するインフラの提供”

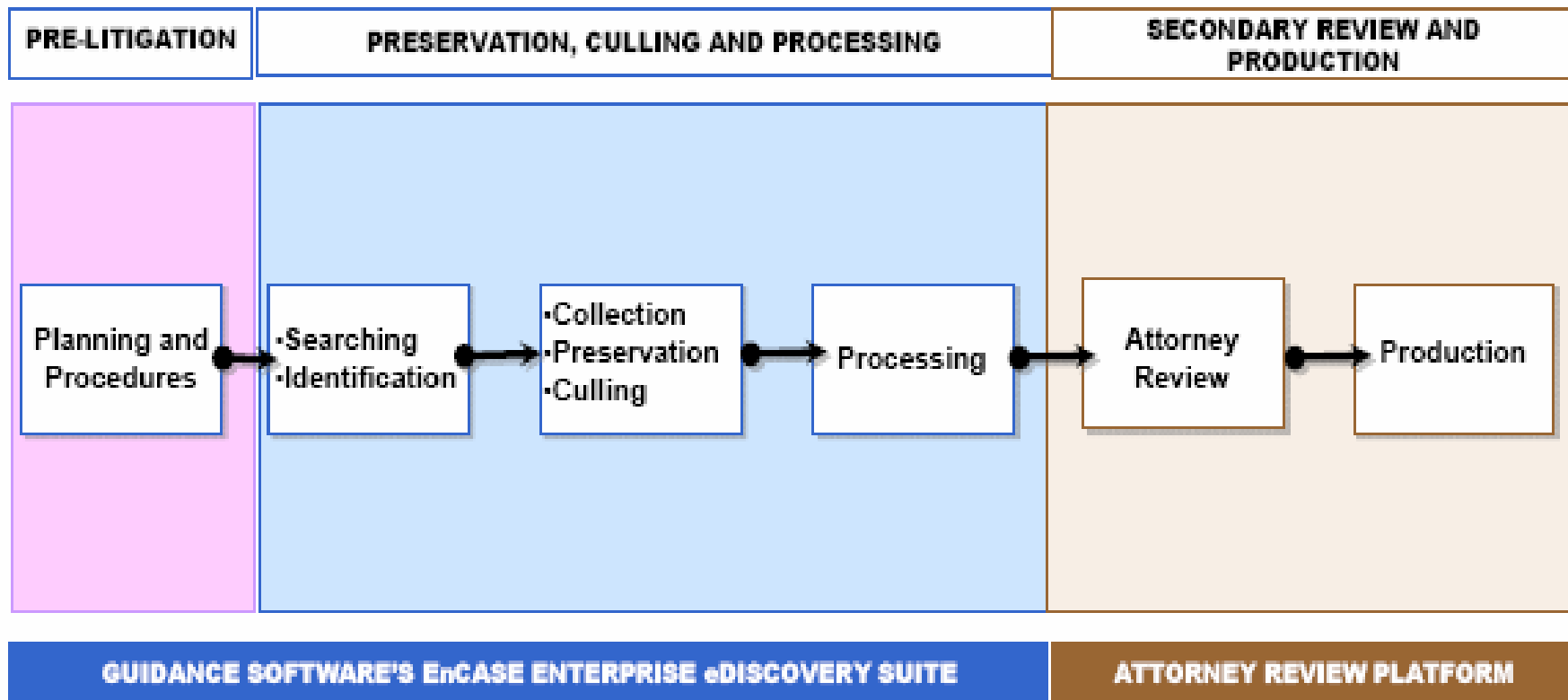


政府、捜査機関、科学、金融、製造、流通、食品、情報、サービス業 etc.

# 米国SOX法のポイント(内部調査インフラの構築の必要性)



- 内部調査・内部統制監査インフラ構築（302条,404条&806条）
- デジタル証拠取得・保全能力（301条, 302条&404条）
- 証券取引委員会(SEC)、FBI、警察との協力体制の確立（Ex.Act #44969）
- 虚偽発生リスクに迅速な対応体制（302条、404条、409条）
- 証拠保全能力-破壊・消去された文書の回復など（802条）
- 内部統制の不備に関する適宜報告（409条）
- 内部統制の評価（監査）能力の完備（301条）



➡ Data Flow;  
Initial Culling Can Occur with Collection;  
Secondary Culling on Collected Data

- 欧米での民事訴訟ではeDiscoveryが必要
  - デジタルデータの開示が不適切な場合、不利になる可能性が高い
- 廃棄・改ざんの防止
  - デジタルデータの非改ざんを立証する必要がある(改竄には重罰)
- 費用負担 >> 文書保管者側
- 3要素
  - 証拠保全、解析、報告
- 留意点(適切に実施できない場合)
  - 機密情報や不利な情報の流出、信頼性の低下、隠蔽工作の疑い、
- 課題
  - 超大容量(>>関連ファイルのみ抽出)、多種の対象デバイス、文字コード

# 顧客例

**HALLIBURTON**

**DELL™**

**SEI** New ways.  
New answers.®

**ChoicePoint**

**U.S DEPARTMENT of STATE**



**KAPLAN**



imagination at work



STATE STREET.



**Florida's health**  
THE FLORIDA DEPARTMENT OF HEALTH

**McAfee**

「EnCase Enterpriseで、最初の6ヶ月間で\$1Mのコストを削減できた。さらにM&Aに伴う機密情報の迅速で完全な開示を可能にした。他のどんなソフトウェアやサービスをもってしてもそれは不可能」  
(Ted Barlow, CSO & VP of Risk management)

## シノップシス社(Synopsys) e-Discovery(知的財産の流出)

元従業員がIPを盗用し退社後設立したNassda社で競合製品を発売した。裁判は2年以上の長期にわたり、シノップシス社は元従業員の不正を証明する必要があった。多くのコンピュータ・エビデンスが紛失あるいは消失していたが、EnCase Enterpriseを使用して詳細に調査した結果、シノップシス社の機密情報と同一のドキュメントをNassda社のネットワークから抽出できた。結果シノップシス社は\$61Mの和解金を受け取ると共に、Nassda社の買収が認められて事態を収拾。

## ハリバートン社(Halliburton) e-Discovery

電力・ガス設備のトップ企業で各国で行政の規制・監視下にあり多くの公共・民間訴訟を受けていた。件数の多い中小規模の訴訟では1件あたり20万～100万ドルのeDiscovery費用がかかり、年間で数1000万ドルの費用が発生していた。EnCase e-Discoveryを導入により費用削減額は年間1000万ドル(10億円)規模に達している。

## 大手SI会社 インシデント・レスポンス

2000台のサーバーが侵入を受け機密情報盗難の危機にあった。Ernst & Youngに調査を受託しEnCase Forensicで作業を開始したが、手作業のため30台のサーバーに焦点を当てた作業しかできず3週間後に何も発見できなかったことを報告し、謝罪した。次にガイダンスのプロフェッショナルサービス部門が調査依頼を受け、EnCase Enterpriseで2000台のサーバーすべての調査を2週間で行った。その結果ハッカーの侵入方法やデータへのアクセス方法、被害を受けたサーバーの特定化ができた。

## 米国財務省 Fraud(情報漏えい)

情報漏洩の疑いで1750台のPCを対象に1.5テラバイトのNovellファイルと120の大規模PSTに調査。当初\$3.5MをかけてSIIに作業委託したが9ヶ月間で全体の10%しか調査できず、結果も不正確で断念。その後EnCase Enterpriseで再調査し5週間ですべての調査を完了。財務省は事例に協力。

# Case Study-1:

## ■ **Situation:**

- Network Associates had contracted to sell its Sniffer Technologies Unit for \$275 Million.

## ■ **Issues:**

- The contractual terms required Network Associates to ensure that none of the tool's source code remained on Network Associates' computer systems.
- 5000 computers in 20 different locations worldwide totaling approximately 100 TB.

## ■ **Solution:**

- Using EnCased Enterprise forensic technology, NA could sweep systems around the clock.
- Located 40 drives that contained source code; eradicated the files and got government approval.

# Case Study-2:

## ■ **Situation:**

- Data had leaked from Classified Network to Unclassified Network

## ■ **Issue:**

- 1600 workstations totaling approximately 13 TB in aggregate and 2 terabytes of additional stored data required to be searched for the leaked data
- 100% confidence in the discovery and isolation of leaked data due to congressional oversight
- Exposure and control of search terms
- Prior vendor had spent approximately 3 months and \$1 Million to complete only 3 TB

## ■ **Solution:**

- Isolation and remediation was completed in 3 weeks; came in \$150K under budget; total cost less than \$500K.

# Case Study-3:

## ■ Situation:

- Halliburton is subject to regulatory oversight by governments around the world, as well as litigation actions by myriad public and private interests.
- There are over 90,000 employees with computer systems, many large file and application servers.

## ■ Issues:

- To maintain a strong corporate position, Halliburton will settle cases only on the merits, not on cost to defend itself.
- Numerous small to midsize lawsuits cost \$200,000 to \$1 million each in eDiscovery vendor fees.

## ■ Solution:

- Using a forensic infrastructure, small, medium and even large eDiscovery matters can be handled in-house.
- Net savings are on the order of \$250,000. The aggregate cost savings are in the millions of dollars annually.

# 基本コンポーネント

Encase Enterprise により、顧客は自らは、他顧客とは異なる環境にセキュアな環境で、エンコープドおよびデコープドされたイベントを調査することが可能になります。100%の完全制御を維持してデータを保護し、すべての疑念と問題を迅速に解決（公衆網通信）上の疑念をホームで解決されます。基本コンポーネントでは、次の内容が提供されます。

**Encase ソフトウェア** - 調査と関連するデータを調査する目的でシステムにインストールされます。

**SQL (Secure Authentication For Encase)** - ユーザーの認証、アクセス権の管理、Encase トランザクションの管理、セキュアなデータを保護可能なサーバー。  
**SQL は暗号化データ ストリームを使用して、Encase およびサードパーティ コンポーネントを通信します。**

**サーバー - サードパーティの製品および環境を統合する、ワークステーションおよびサーバーにインストールされるエージェント ソフトウェア。**



ENCASE ENTERPRISE

次世代インシデントレスポンスソリューション

企業運営に情報は不可欠であり、あなたはその情報の保護に携わっています。ただし、さまざまな種類の攻撃元が存在し、マニュアル的な対応では特定が困難です。

# 製品の特徴

EnCase Enterprise は調査対応型のインフラストラクチャを提供し、ネットワーク上で動作するコンピュータの状態に関する詳細な調査を可能にします。この調査により、コンピュータがどのような処理を実行しているか、不正プロセスを実行しているかどうか、不正な通信に参与しているかどうかといった点が明らかになります。このソリューションはルートキット、トロイの木馬、ワーム、およびその他の悪意のある攻撃について警告し、ネットワークの安全を維持します。

EnCase Enterprise はセキュリティと信頼性に優れたプラットフォームであり、複数のオペレーティング システム上で機能し、最大規模の組織のニーズに対応できます。

**既存のセキュリティ投資を最大限に活用**  
IDS (侵入検知システム) や SMS (セキュリティ情報管理システム) から 1 日に発生される警告の数は、数百から数千件に達します。ただし、どの警告が実際の危険を通知しているのかを把握するのはほぼ不可能に近く、すべての警告の過剰および分析に対応できるリソースは組織には存在しない状況です。担当者が手動で個別のツールを使用して警告の重要性を把握する際には、遅い対応が手遅れになっています。つまり、事象が発生した時点から対応の準備が整うまでの間に、対応に必要な情報が陳腐化するか、そのまま失われてしまっているのです。

EnCase Enterprise は、IDS とその他のセキュリティ監視システムをスムーズに統合し、警告が受信された時点で、リアルタイムの自動インシデントレスポンス プロセス「Snapshot」をトリガします。ソースおよびタ

ーゲットから得られた情報の即時分析により、既知/不明/隠しプロセス、TCP ネットワーク ソケット情報、開いているファイル、デバイス ドライバ、サービスなどの詳細が明らかになり、コンピュータが危険な状態であるかどうかが可能になります。タイム スライス単位で攻撃的な活動が判明した直後に Snapshot がトリガされ、イベントが実際に発生したかどうか、発生した場合はその影響と原因が明らかになります。

自動警告調査機能により、複数の情報源から重要なすべてのイベントに対応することが可能になります。

**面倒で時間のかかる作業を自動化** - 攻撃の発生が確認された場合、EnCase Enterprise は社内全体のコンピュータに対して確実性の高い分析を自動的に行って、同じワーム、ゼロデイ攻撃、およびトロイの木馬に感染している他のコンピュータを抽出できます。このソリューションは、攻撃の特性を示す署名や「指紋」を初期 Snapshot から収集し、該当する同じ ID をすべてのコンピュータ上で検索します。各コンピュータの詳細なレポートには、実際に発生している事象や危険の原因に関する特定の情報が示されるため、一定の時間を節約できます。EnCase Enterprise は環境の定期的なスキャンにも対応し、内容が類似する危険について予防的な識別や警告を可能にします。IT スタッフおよびセキュリティ調査担当者は、個別のコンピュータを直接調査して、新しいインシデントや過去のインシデントから受けた損害の評価および修正を行うといった、時間のかかる作業を省くことができます。

## 拡大するその他の脅威に対する保護

最近では、企業ネットワークへの攻撃にルートキットを用いる上級ハッカーが増加しています。このようなツールを用いることにより、侵入者はまったく気付かれることなく自由に行動し、ネットワークそのものを支配してしまいます。ルートキットは時間の経過とともにその悪意が高まると同時にさまざまな攻撃で用いられ、顧客情報を盗み出してハッキング先の企業に全額を不当に要求する攻撃者にとって最適なツールとなっています。最近まで、Windows ベースのルートキットはまったく検出できませんでした。EnCase Enterprise は、このような脅威の検出および修正に対応できる唯一の商用ソリューションです。オペレーティング システムを詳細に監視し、ハッカーがどのような手段で自分の身元を隠しているとしても、ルートキットによって使用される隠しプロセスやフックを識別して破壊します。

## あらゆる攻撃に迅速かつ効果的に対応

コンピュータに対する攻撃を把握し、その範囲の拡大を防ぎ、被害の回復を進める上で、迅速な対応が重要になります。コンピュータのハード ドライブから静的データを取得する処理に加えて、EnCase Enterprise Snapshot 機能は RAM に保存された揮発性データまたはライブ データの回収を行います。ネットワークに接続するハッカー、ワーム、およびルートキットを識別し、被害が拡大する前に対応を進める上で、これらの情

報は不可欠です。EnCase Enterprise は、インシデント レスポンスおよび危険性の評価を自動化します。20 種類を超えるソフトウェア ツールの機能が単一のセキュアなエンタープライズ製品に統合され、1 時間にコンピュータ 10,000 台を評価します。このアプローチは、コンピュータ インシデントの処理について、SANS (System Administration, Networking and Security Institute) および NIST (米国家標準技術局) によって設定された標準やベスト プラクティスに沿った標準の再現プロセスを提供します。

## 詳細な分析の実施により防御を強化

EnCase により、セキュリティ分析担当者は、インシデント レスポンスの一環として必要となる、脆弱なコンピュータに対する詳細な分析を行うことが可能になります。改変または削除されたファイル、ホストへの攻撃に使用されたツール、侵入者が環境で活動した期間など、全体を網羅する監視機能によって弱点の識別が可能になり、将来的な攻撃に対する保護が実現します。

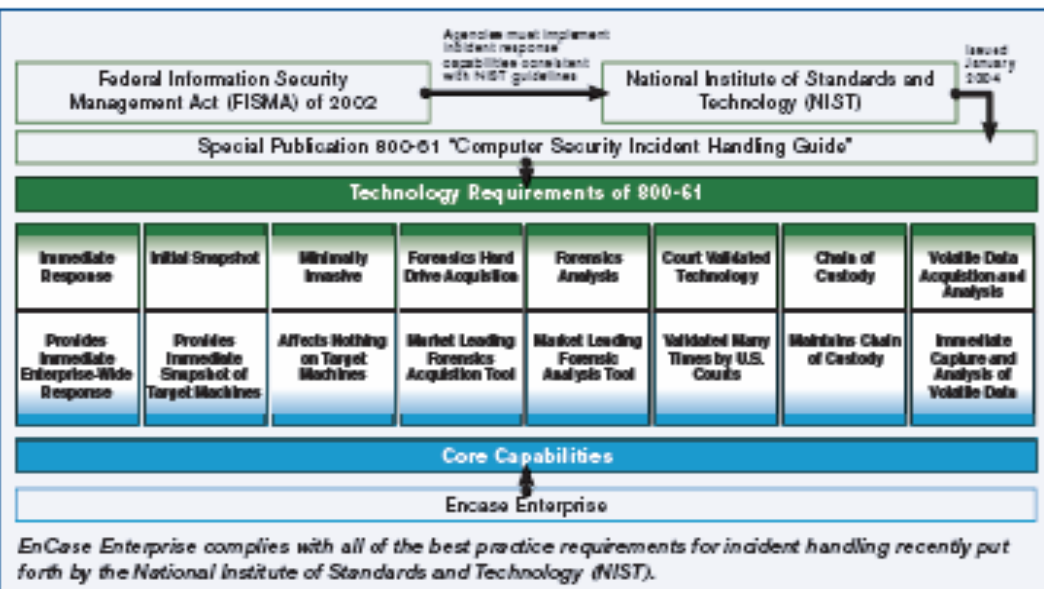
## 包括的なソリューションがもたらす利点

Guidance Software のトータル ソリューションには、高度なインシデント プログラムの構築や既存プログラムの調査を支援する専門サービスが用意されています。

このソリューションは、企業の実績に応じた展開が可能のため、担当者の作業時間を速やかに削減します。弊社の専門コンサルタントは、企業環境に対する重大な脅威の識別、作業を自動化するスクリプトの開発、およびインシデントに対する対応の改善を支援し、これらの要素を詳細なインシデント レスポンスの方法論に取り入れています。また、IDS ツールや SIM ツールを EnCase Enterprise と完全に統合します。最終的に、知識移管アプローチの一環として、弊社は豊富な情報をスタッフに提供し、新機能について経営陣に紹介します。

## 世界レベルの専門家から学ぶ

高度なスキルを備えた IT 専門家に対する需要が高まっているため、最新のインシデント レスポンス テクノロジーと調査対応プロセスについて十分に理解できるように、弊社は調査担当者向けのトレーニングを提供しています。数千人に及ぶ企業やフォレンジック ラボが Guidance Software 社の高度な教育サービスおよび教育方式を採用しています。弊社のトレーニング プログラムは業界トップレベルの講師による指導を特徴とし、企業調査のより効果的な実施を可能にする、インシデント レスポンスに関する基本クラスと上級クラスを提供します。職別別の各クラスは、企業の調査担当者およびコンサルタントに特化して設定されています。



## ガイダンス・ソフトウェアInc. 日本事務所

吉田次男 [tsugio.yoshida@guidancesoftware.com](mailto:tsugio.yoshida@guidancesoftware.com)

ブライアン・デュゲイ [brian.dugay@guidancesoftware.com](mailto:brian.dugay@guidancesoftware.com)

横浜市西区みなとみらい2-2-1 横浜ランドマークタワー20F

TEL : 045-670-7035