第18回
サイバー犯罪に関する白浜シンポジウム
「サイバー犯罪の抑止とダメージコントロール」

ダメージコントロールにおいて SIEMが担うべき役割の重要性

2014年5月24日

日本ヒューレット・パッカード株式会社
BITA（ビジネスーIT・アラインメント）エヴァンジェリスト
佐藤　慶浩

自己紹介

佐藤　慶浩（さとう　よしひろ）　　http://yosihiro.com/

日本ヒューレット・パッカード（株）
チーフ・プライバシー・オフィサー
（兼）BITA（ビジネスーIT・アラインメント）エヴァンジェリスト
元　内閣参事官補佐（民間併任）
　（内閣官房情報セキュリティセンター　情報セキュリティ指導専門官）

【社外の活動】

IT総合戦略本部パーソナルデータ検討会技術検討ワーキンググループ　構成員
厚生労働省　医療等分野における番号制度の活用等に関する研究会　構成員
経済産業省 IT融合フォーラム パーソナルデータワーキンググループ　元構成員
杉並区　住基ネット運用監視委員会　委員長
JIPDEC　プライバシーマーク推進センター　非常勤研究員
JIPDEC　ISMS適合性評価制度技術専門部会　委員
ISO/IEC JTC1/SC27 WG5 プライバシー小委員会　元主査、現エキスパート
情報ネットワーク法学会　前副理事長
デジタル・フォレンジック研究会　理事

【その他】

http://yosihiro.com/profile/resume.html

サイバー犯罪による被害が深刻になる中で企業における
SIEM(Security Information and Event Management)の構築と運用
が不可欠になってきました。
被害発生を前提にすることは受け入れがたく、被害発生を想定
して、その対応を前提にする取り組みが求められています。
そのように被害を最小限にするダメージコントロールがある一方
で、自社による犯罪についての監視も必要です。
企業としての不正が発覚したにもかかわらず、会社上層部が社
内の犯罪行為の有無を捜査機関より迅速かつ詳細に調査でき
ず、米国有数の大企業が解散にまで追い込まれて世界を震撼さ
せたことがあります。
企業にとって解散は最大のダメージですが、喉もと過ぎて、そこ
からの教訓に学んでいないようにも思われます。
組織内での被害だけでなく不正行為の有無など業務全般を広く
監視することでSIEMへの投資対効果を高め、情報セキュリティ課
題から経営課題に昇格させる必要性について紹介します。

総合的なリスクマネジメントには SIEMの実現が必要です

Defined by GartnerGroup

SIEM = SIM & SEM　セキュリティ情報、イベント管理

SIM : Security Information Management

事後調査型
フォレンジック

- ✓ ログマネジメント機能
  （ログ＆イベントデータの効率的な蓄積、分析）
- ✓ ユーザ・リソースアクセス分析 （ユーザアクセスのポリシー違反・例外抽出）

SEM : Security Event Management

即時性、相関
モニタリング

- ✓ リアルタイムイベントデータ収集、セキュリティイベントコンソール
- ✓ リアルタイムイベント相関分析（モニタリング、通知アラート）
- ✓ インシデント管理サポート

温故知新

侵害行為の類型

許可されていない者による侵害行為（いわゆる外部犯）

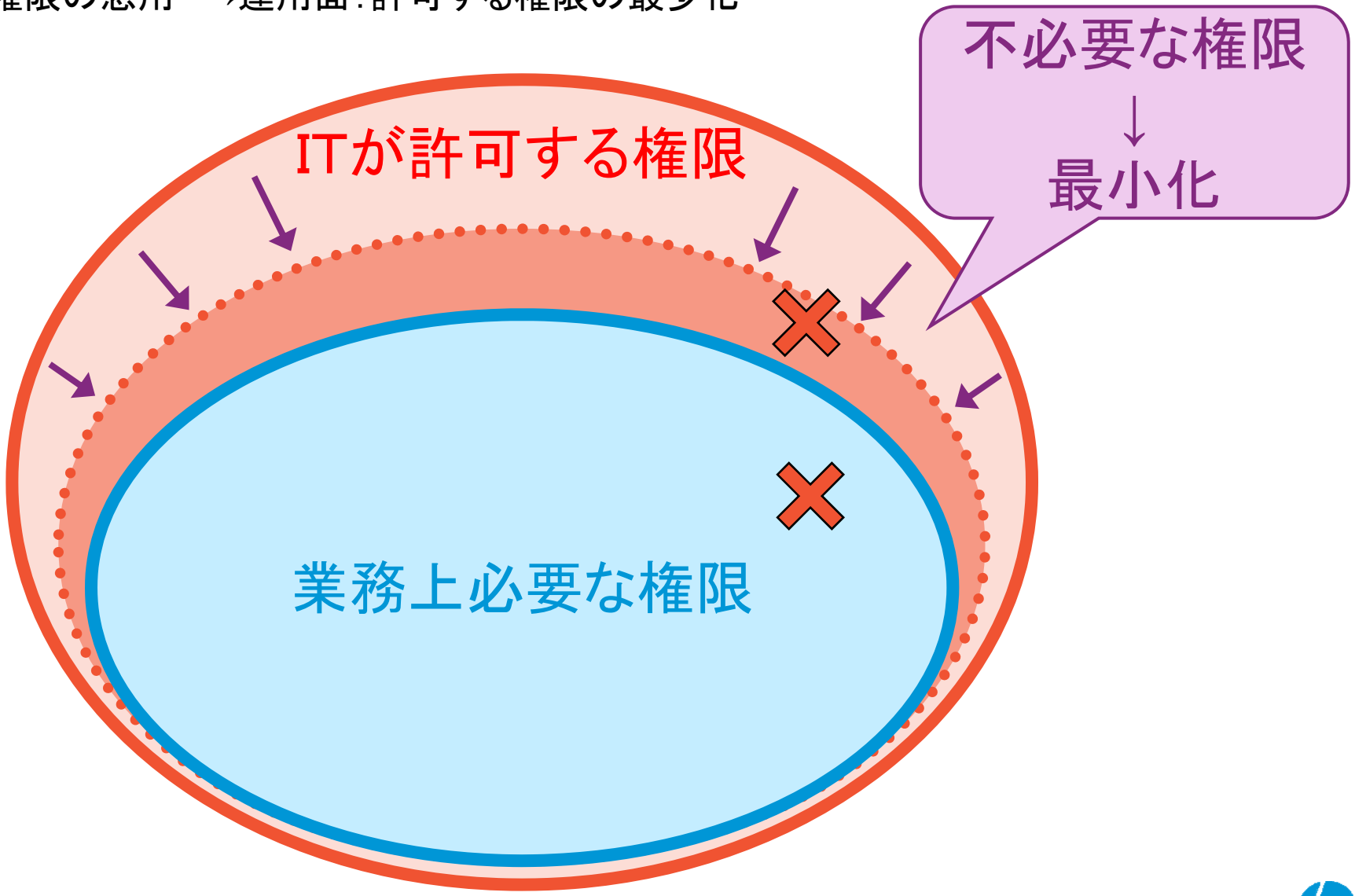
- 無許可の行為　悪意あり
  - 技術面：アクセス制御による防御・多重の防御

許可された者による侵害行為（いわゆる内部犯）

- 誤操作・過失　悪意なし
  - 誤操作を軽減する設計
  - 啓発、教育、訓練
- 権限の悪用　悪意なし　悪意あり
  - **許可する権限の最少化**
  - 監視による抑止効果
  - アノマリ・アクセス（非通常行動）の検出

侵害行為の類型

→権限の悪用　→運用面：許可する権限の最少化



侵害行為の類型

許可されていない者による侵害行為（いわゆる外部犯）

無許可の行為　悪意あり

技術面：アクセス制御による防御・多重の防御

許可された者による侵害行為（いわゆる内部犯）

誤操作・過失　悪意なし

誤操作を軽減する設計

啓発、教育、訓練

権限の悪用　悪意なし　悪意あり

許可する権限の最少化

監視による抑止効果

➡ アノマリ・アクセス（非通常行動）の検出

テキスト

・メール
・PDF
・言語非依存

音声

・Speech to text
・話者の特定
・言語非依存

動画

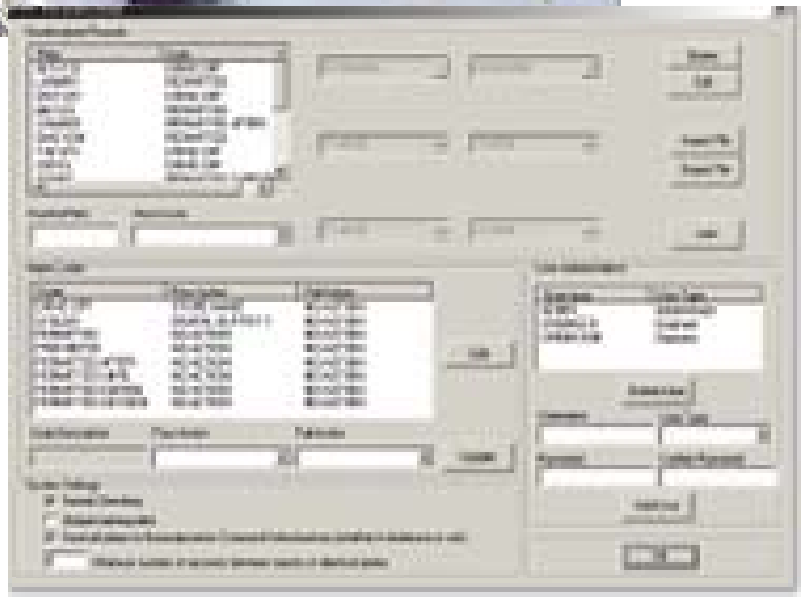
・Speech to text
・数字テロップ認識
・顔認識

画像

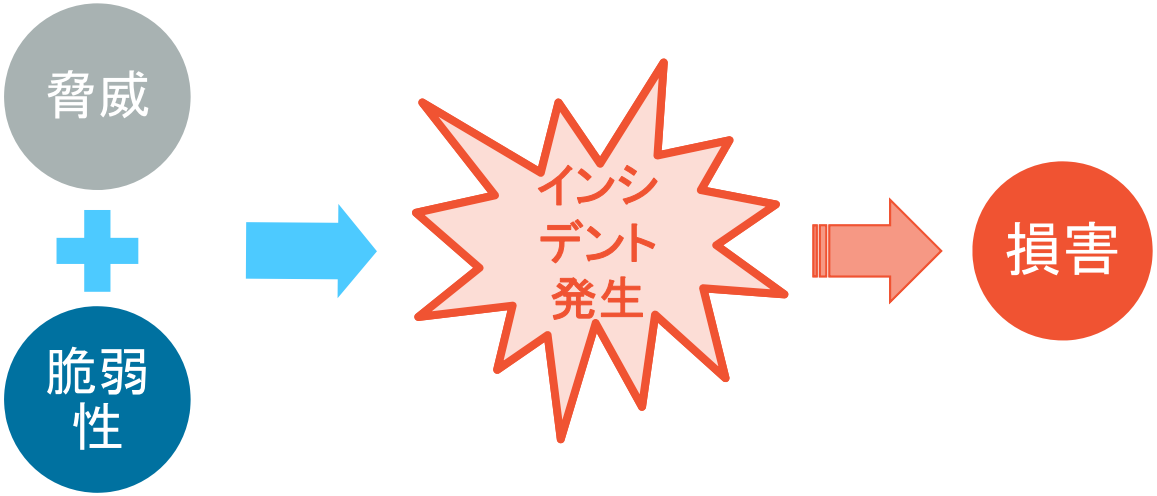
・数字、テロップ認識
・顔認識

紙文書

・OCR



SIEMへの取り組み
発見的対策の導入及び、リアルタイム・モニタリングの実現



予防的対策

抑止　予防

主に発生可能性の低減

- ID管理(AD)
- 構成管理、バージョン管理、バックアップ管理
- ネットワークセキュリティ管理
（FW,WAF,Proxy,IPS etc.）
- アプリケーション管理
- エンドポイント管理

発見的対策

検出　回復

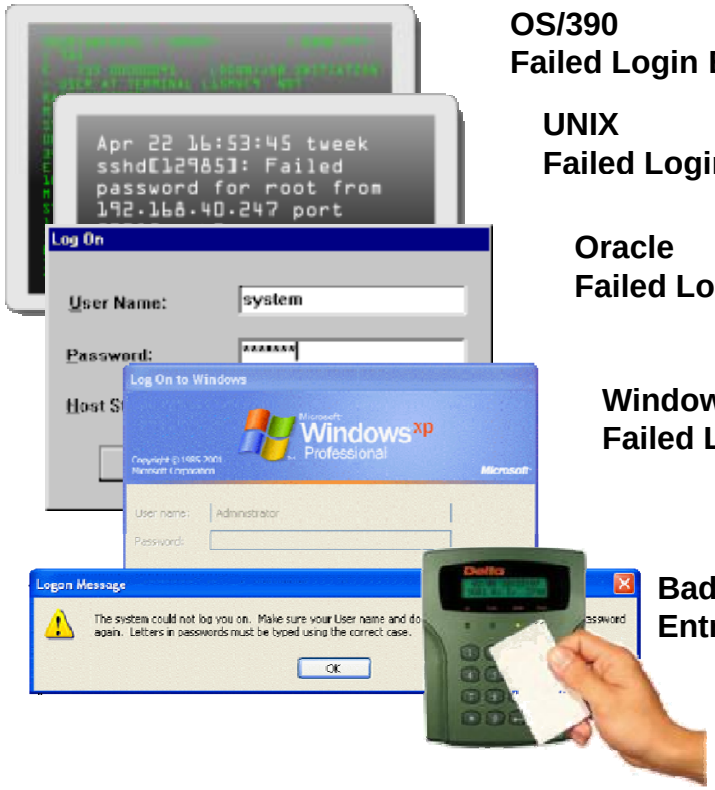
損害の低減

- モニタリング監視
（グレーゾーン/アノマリーetc.）
- インシデント管理

最終的に損害を最小化すために
最適なバランスを考慮したセキュリティ対策が必要

シンプルに

製品が異なると、同じ意味でも異なるメッセージが出力されるため、各製品に詳しい人しかログ内容を理解できない



OS/390
Failed Login Event

UNIX
Failed Login Event

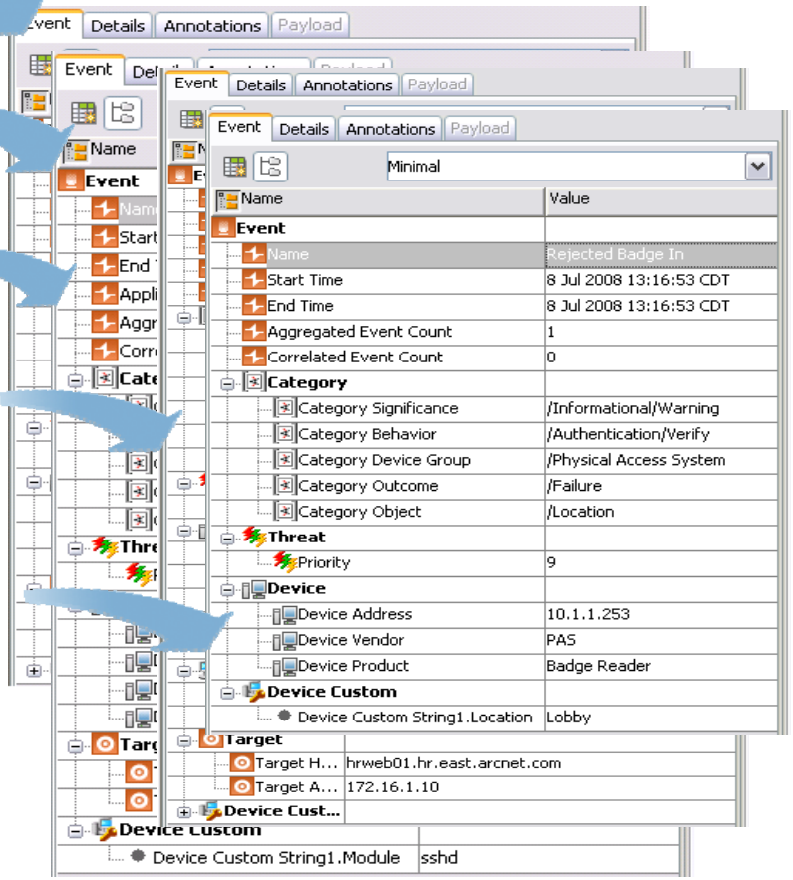
Oracle
Failed Login Event

Windows
Failed Login Event

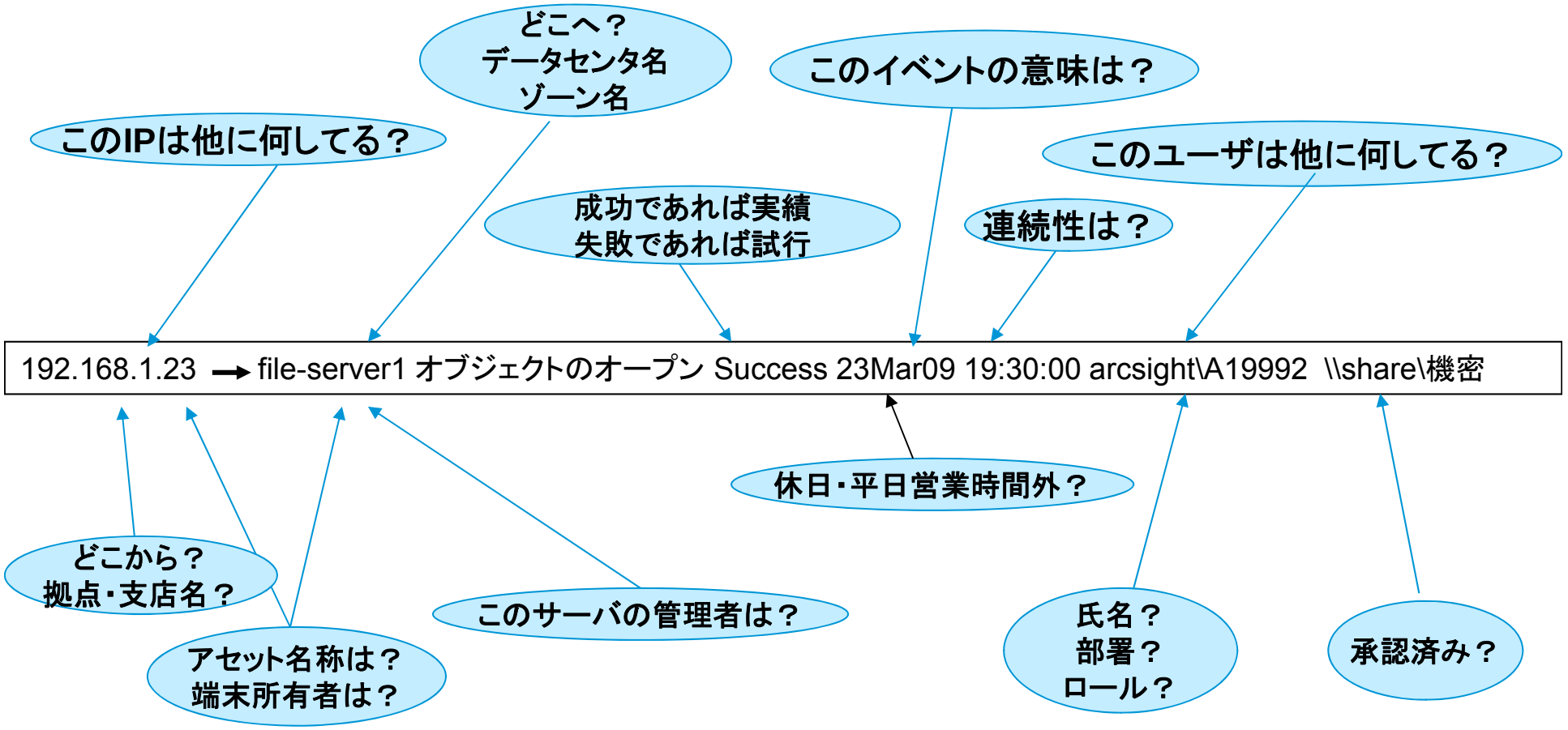
Badge Reader
Entry Denied

すべてのログデータに共通化した属性を付与

正規化されたイベント：***Login Failure***
カテゴリ：***Operating System***



インテリジェントに



効率的に

押収 → 押収物の仕分け → 証拠発見 → 証拠レビュー・提出

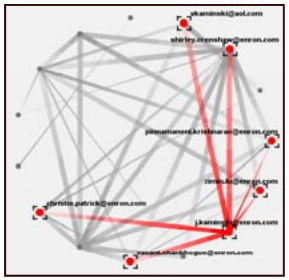
メール

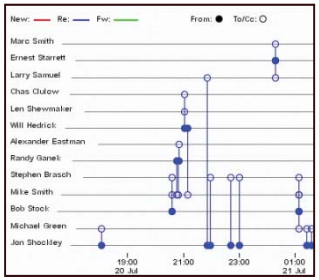
データベース

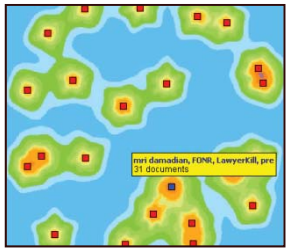
電話録音

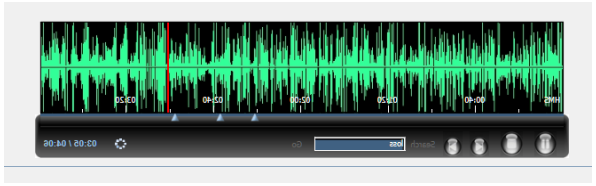
紙文書

インデックス付け
検索を可能に

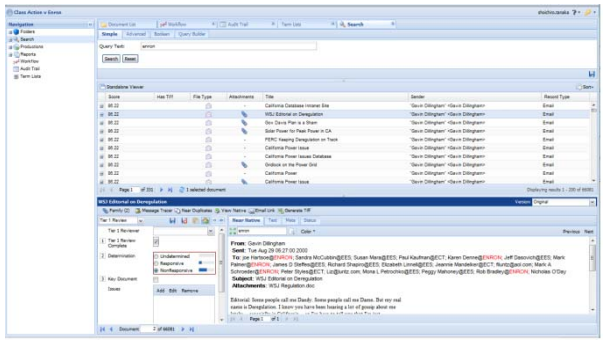








証拠物件のチェック
ワークフロー



マネジメントする

【一元管理】

イベントソース

- PC
- Network Devices
- Servers (UNIX, Linux, Windows…)
- AS/400 Mainframe
- Data Base (Oracle, DB2…)
- Business Applications

参照情報

- 脆弱性管理DB
- Security Intelligence（指令サーバのドメイン情報等）

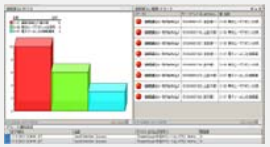
SIEM SYSTEM

【分析とレポーティング】

①即時アラート

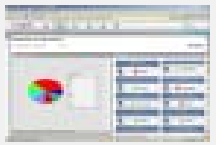
- 攻撃の疑いが検知された場合、その事実を直ちにメール等で通知されます。
- 通知に基づき、攻撃への迅速な対応、被害の最小化を行います。

②ダッシュボード



- システム上で発生しているイベントのサマリ情報をダッシュボード形式でリアルタイムに確認します。
- 必要に応じて個々のイベントをドリルダウンし、詳細を確認します。

③定期レポート



- 日次/週次/月次等の頻度で、攻撃の兆候や発生に係る定期レポートを出力します。
- 定期レポートを基に、現状の対策の有効性や、今後実施すべき対策について検討を行います。

【インシデント管理・ステータス管理】

- 即時アラート、ダッシュボードまたは定期レポートで攻撃の疑いを検知した場合、関連部門と連携し、調査を行います。
- 調査のステータス及び調査結果を一覧管理します。

SIEM
Security Information & Event Management

SIEMを成熟させるには
シンプルに
インテリジェントに
効率的に
マネジメントする

SIEM needs
Simple, Intelligent and Efficient Management

あらゆる構造データと非構造データをインデックス付けし、マーケティング、訴訟対応などに活用

発表資料のダウンロード

http://yosihiro.com/speech/#2014-05-24