サイバー攻撃や内部不正に対して企業はどう立ち向かうべきか

IBM Computer Security Incident Response Team
IT Forensic Analyst
守屋　英一

注意：この資料の掲載内容は私自身の見解であり、必ずしもIBMの立場、戦略、意見を代表するものではありません。

■名前　守屋英一

■経歴

2007年より、日本アイ・ビー・エムに入社
2001年より、インターネット・セキュリティ・システムズに入社

■活動

日本シーサート協議会運営委員及び、インシデント事例分析WGリーダー
中央大学大学院 戦略経営研究科 戦略経営専攻
明治大学 ビジネス情報倫理研究所 客員研究員
JNSA　SNSセキュリティWG　メンバー（2012年）
不正アクセス防止対策に関する官民意見集約委員会委員（2012年）
経済産業省　CTAPP　運用・技術WG構成員（2012年）
内閣官房情報セキュリティセンター「ウイルスの振る舞い分析」構成員（2010年）
サイバークリーンセンター研究員（2007年）

■著書

2014年5月13日「ネット護身術入門」（朝日新聞出版）
2014年3月13日「サイバーセキュリティ」（NTT出版）
2013年7月20日「フェイスブック情報セキュリティと使用ルール」（あさ出版）
2012年6月20日「フェイスブックが危ない」（文藝春秋）

■受賞

2014年度マイクロソフトMVPセキュリティ部門を受賞
2012年度JNSA表彰個人の部を受賞

責任の分界点が曖昧になっている

技術の発展とグローバル化に加え、ビジネスモデルの変化、雇用形態の変化が進み、責任分界点が曖昧になっている。

出所：
総務省白書平成26年版http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc254110.html
厚生労働省：http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000046231.html
株式会社 ICT総研 http://www.ictr.co.jp/report/20140821000067.html
日経BPコンサルティングhttp://consult.nikkeibp.co.jp/consult/news/2014/0829sp/
矢野経済研究所http://japan.zdnet.com/article/35056740/

サイバー攻撃

高度な手法

陳腐な手法

•大規模攻撃

金銭目的(2003年～)
•無差別なウイルス配布
•スパム
•スケアウェア

情報搾取(2007年～)
•標的型攻撃
•APT **(Advanced Persistent Threat)**

愉快犯(2001年～)
•DDoS攻撃
•ハクティビズム

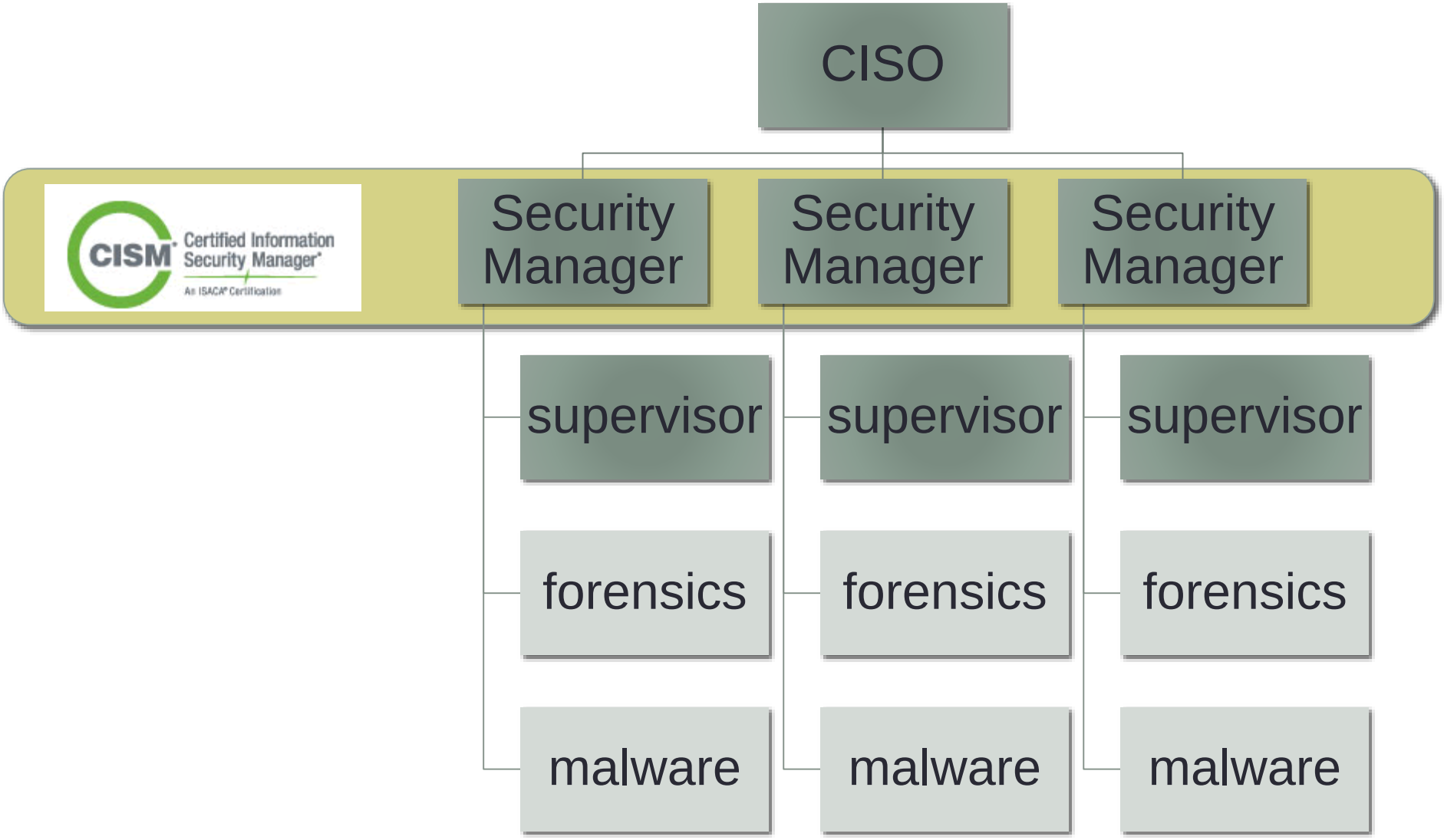
攻撃対象が広範

攻撃対象が限定的

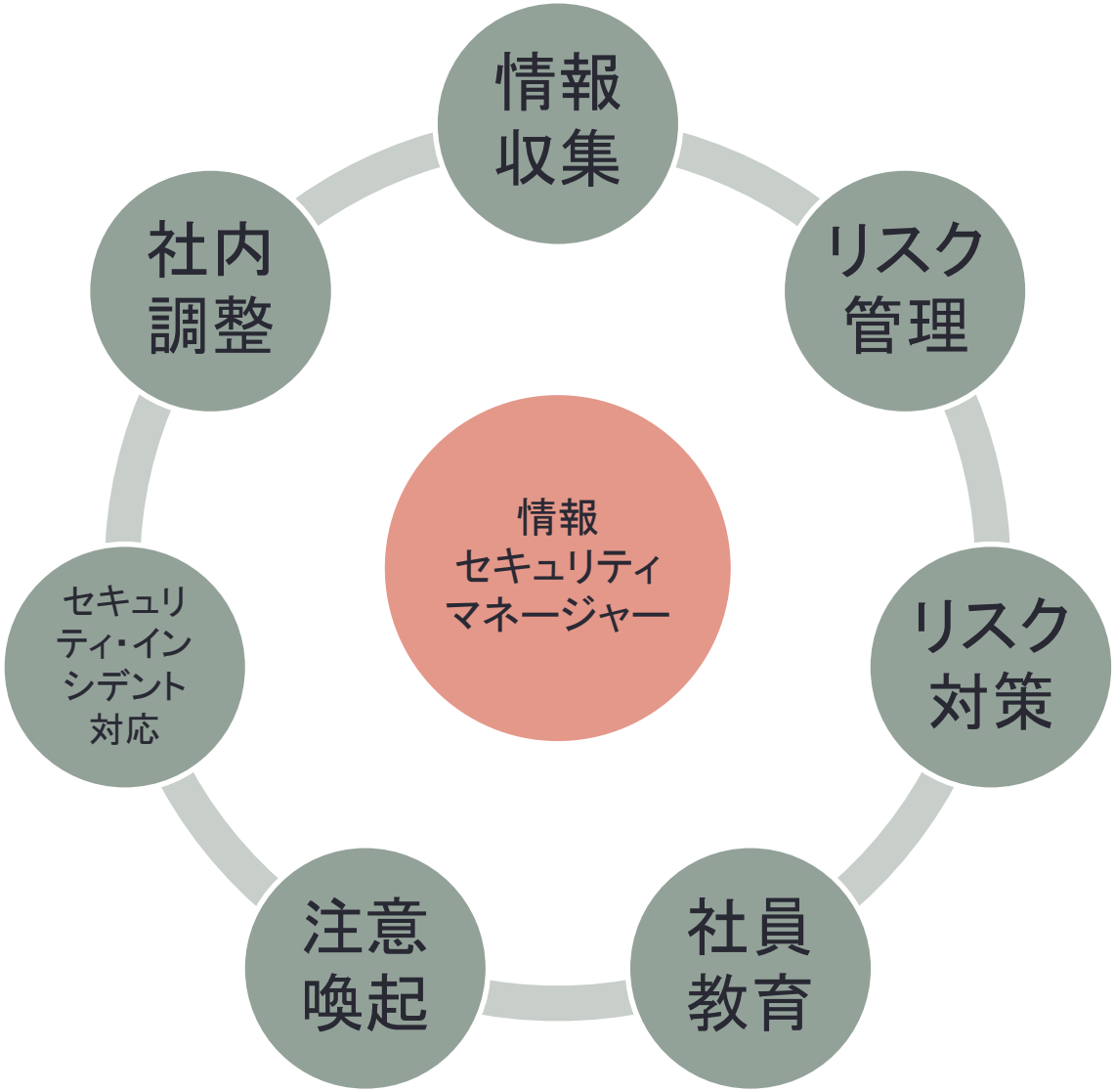
内部不正

	動機・目的	背景・原因
動機づけられた犯罪者	＜金＞ 金銭的動機、経済的動機 ＜怨恨＞ 上司への不満（評価、待遇、給与） 人間関係の不満、不当解雇	＜正社員＞ 終身雇用・年功序列、転職、起業 ＜非正規社員＞ 低賃金、雇用が不安、キャリア形成の貧困化
潜在的な犯行対象物	＜情報＞ 機密情報（知的財産、営業機密） 顧客情報、開発情報、従業員情報 ＜システム＞ システムの破壊、システムの悪用	＜電子データ＞ 大量の情報を持ち出すことが可能 ＜システム＞ 分業化、専門家され、全体把握が困難になっている
監視性の低い場所	＜社外＞ 外部委託先、アウトソーシング先 ＜ルール＞ ルールが存在しない ＜監視＞ 情報の管理が不十分 ルール違反しても処罰されない	＜社外＞ 経営の効率化が図られ、社外への業務移転が進んだ ＜ルール＞ ルール陳腐化が早まっている ＜監視＞ 職務分掌が進んでいない

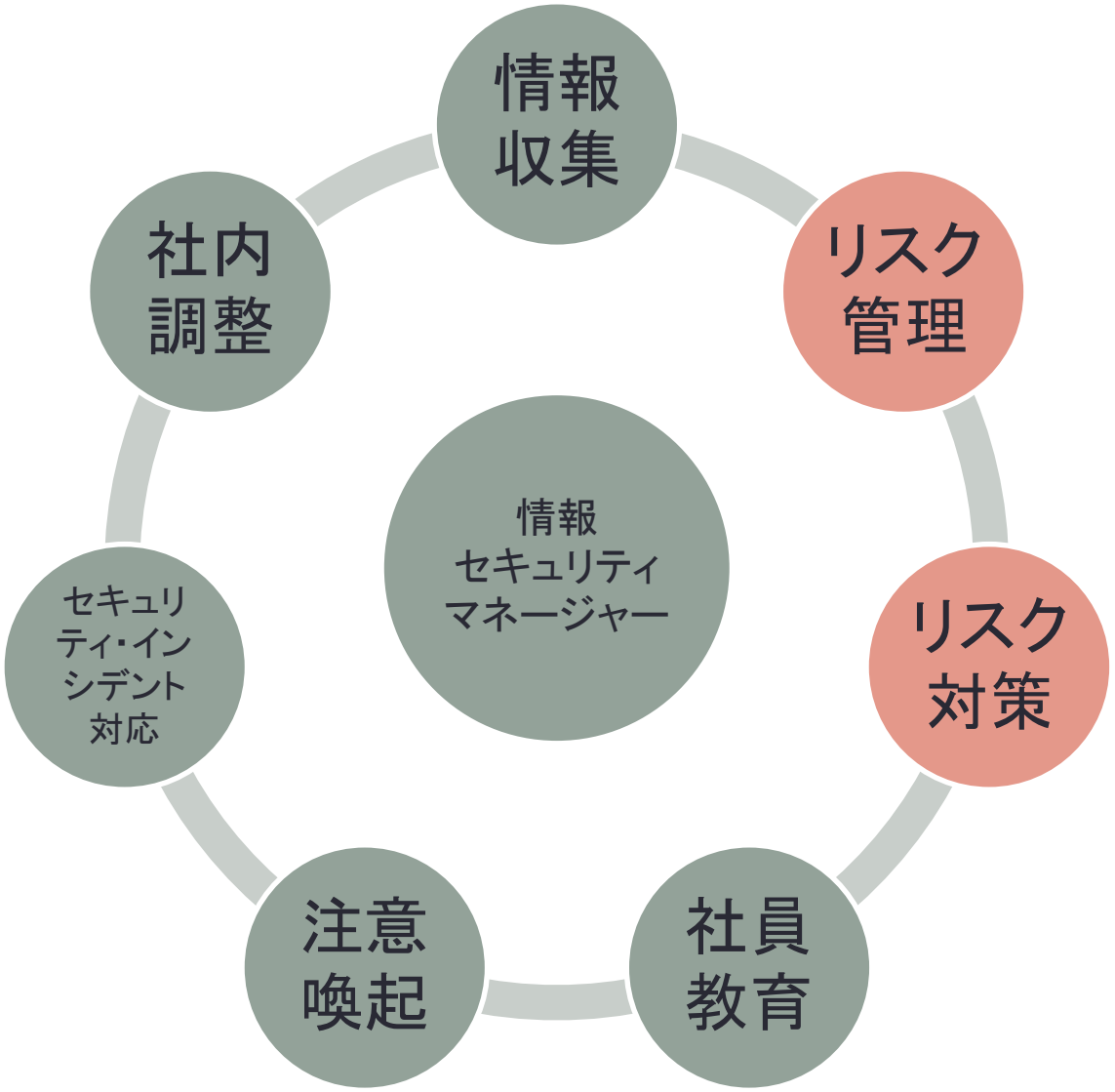
運用体制


CISO
CISM Certified Information Security Manager
An ISACA Certification
Security Manager
Security Manager
Security Manager
supervisor
supervisor
supervisor
forensics
forensics
forensics
malware
malware
malware

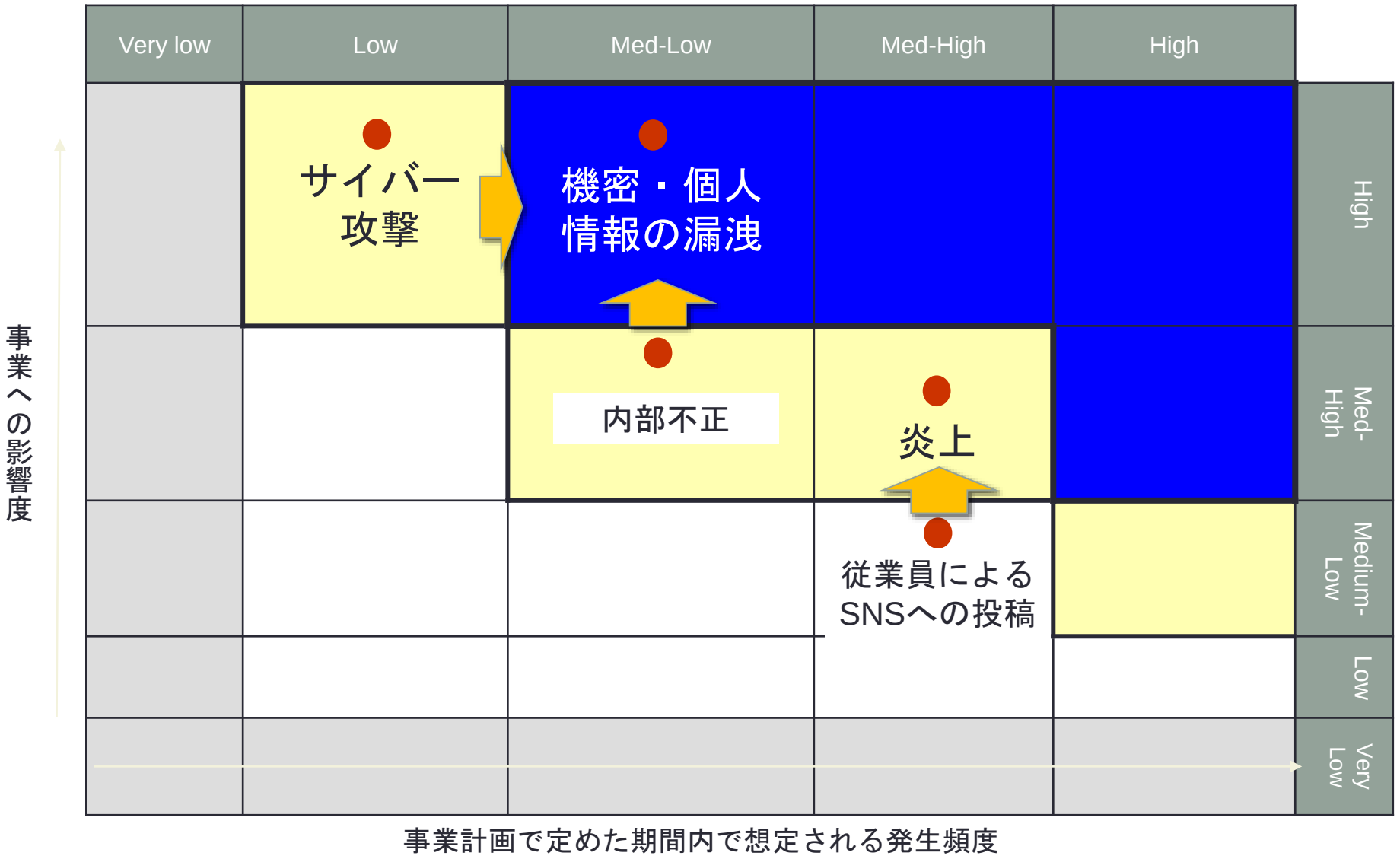
情報セキュリティ部門の業務範囲



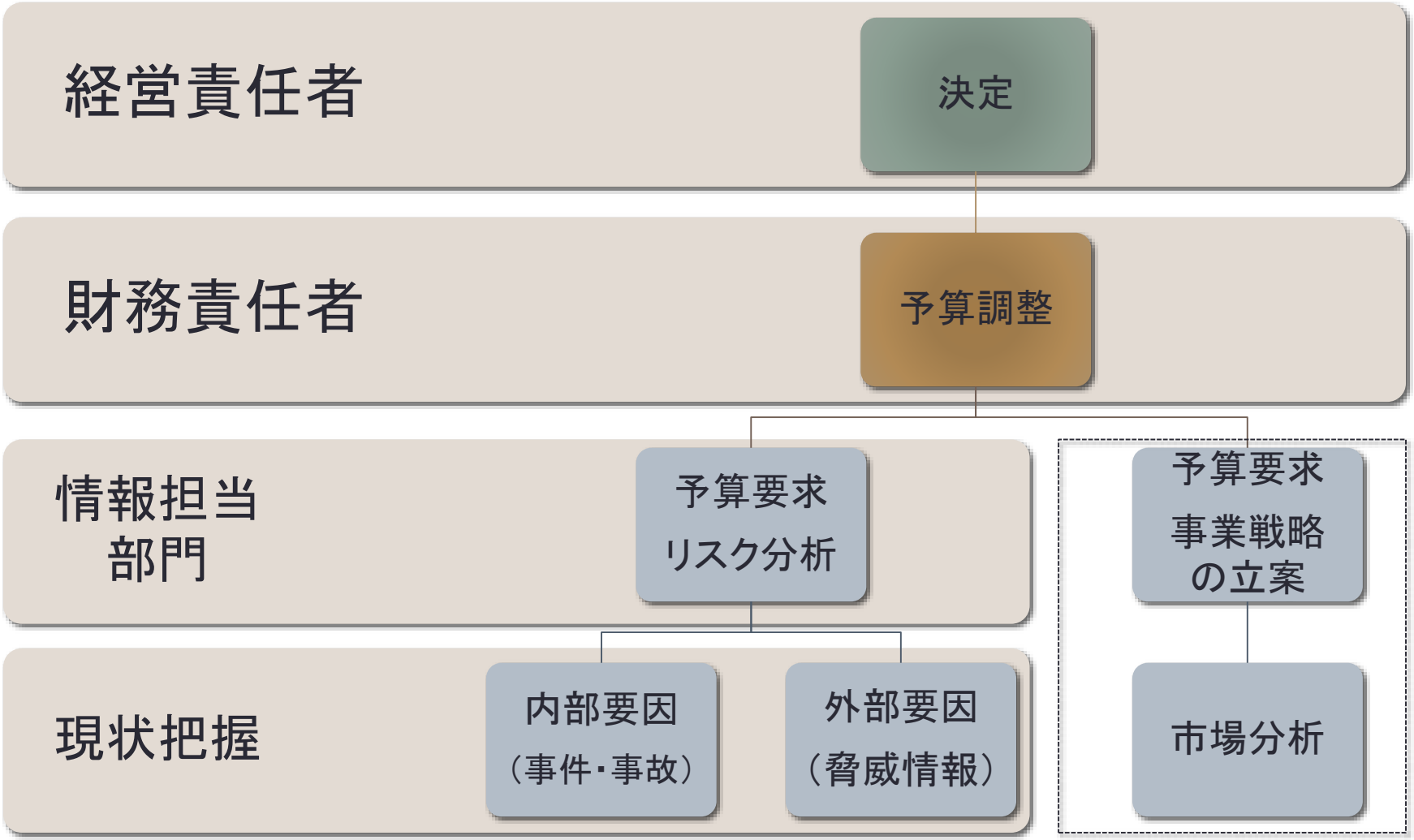
情報セキュリティ部門の業務範囲



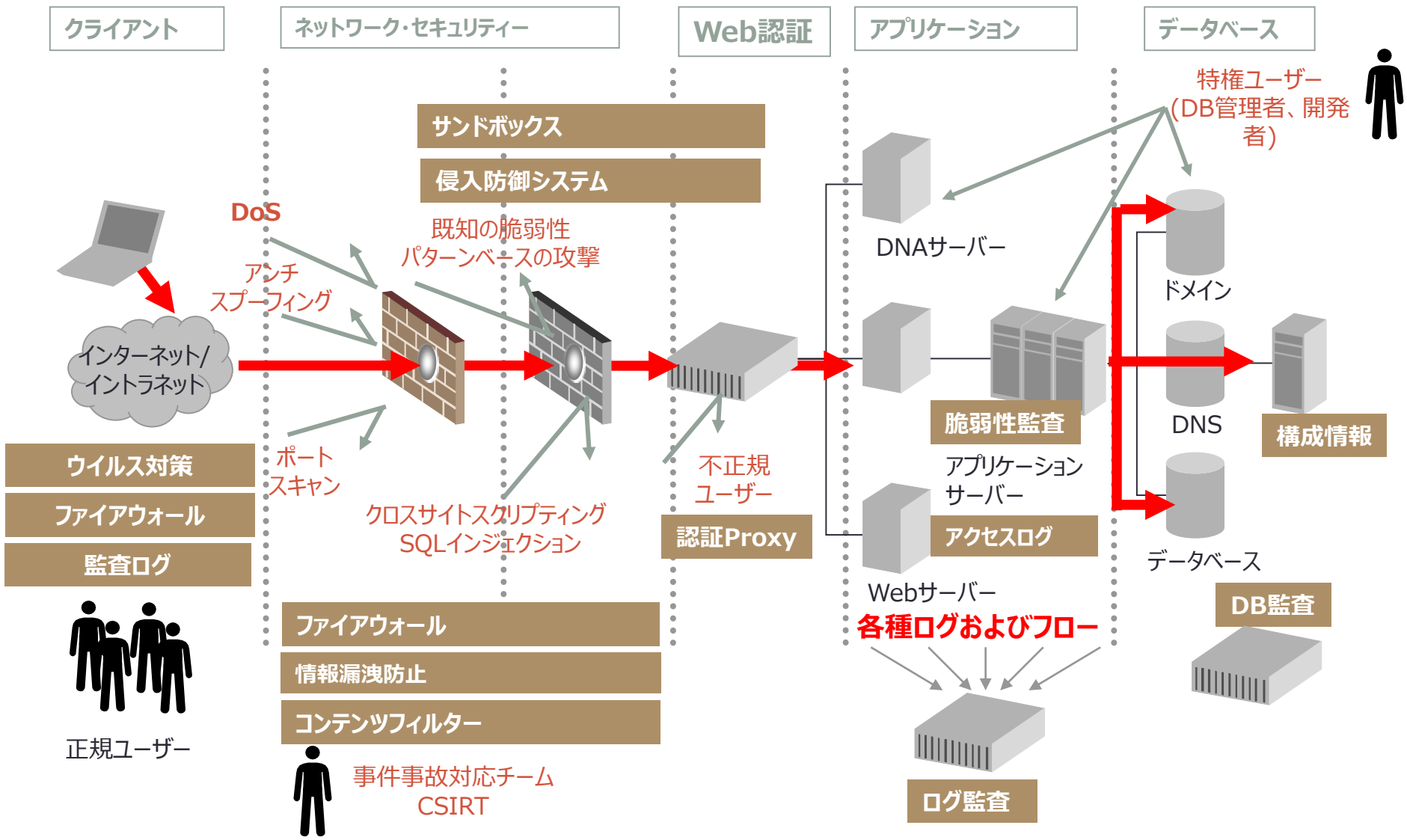
リスクの分析


Very low
Low
Med-Low
Med-High
High
High
Med-High
Medium-Low
Low
Very Low
サイバー攻撃
機密・個人情報の漏洩
内部不正
炎上
従業員によるSNSへの投稿
事業への影響度
事業計画で定めた期間内で想定される発生頻度

予算化


経営責任者
決定
財務責任者
予算調整
情報担当
部門
予算要求
リスク分析
予算要求
事業戦略
の立案
現状把握
内部要因
（事件・事故）
外部要因
（脅威情報）
市場分析

対策の検討


クライアント
ネットワーク・セキュリティー
Web認証
アプリケーション
データベース
サンドボックス
侵入防御システム
DoS
既知の脆弱性
パターンベースの攻撃
アンチ
スプーフィング
インターネット/
イントラネット
ウイルス対策
ファイアウォール
監査ログ
ポート
スキャン
クロスサイトスクリプティング
SQLインジェクション
不正規
ユーザー
認証Proxy
DNAサーバー
特権ユーザー
(DB管理者、開発者)
ドメイン
DNS
構成情報
脆弱性監査
アプリケーション
サーバー
アクセスログ
データベース
DB監査
Webサーバー
各種ログおよびフロー
ファイアウォール
情報漏洩防止
コンテンツフィルター
事件事故対応チーム
CSIRT
ログ監査
正規ユーザー

ブルース・シュナイアー氏　5段階評価法

Ⅰ
- 守るべき資産は何か

Ⅱ
- その資産はどのようなリスクにさらされているのか

Ⅲ
- セキュリティ対策によって、リスクはどれだけ低下するのか

Ⅳ
- セキュリティ対策によって、どのようなリスクがもたらされるか

Ⅴ
- 対策にはどれほどのコストとどのようなトレードオフが付随するか

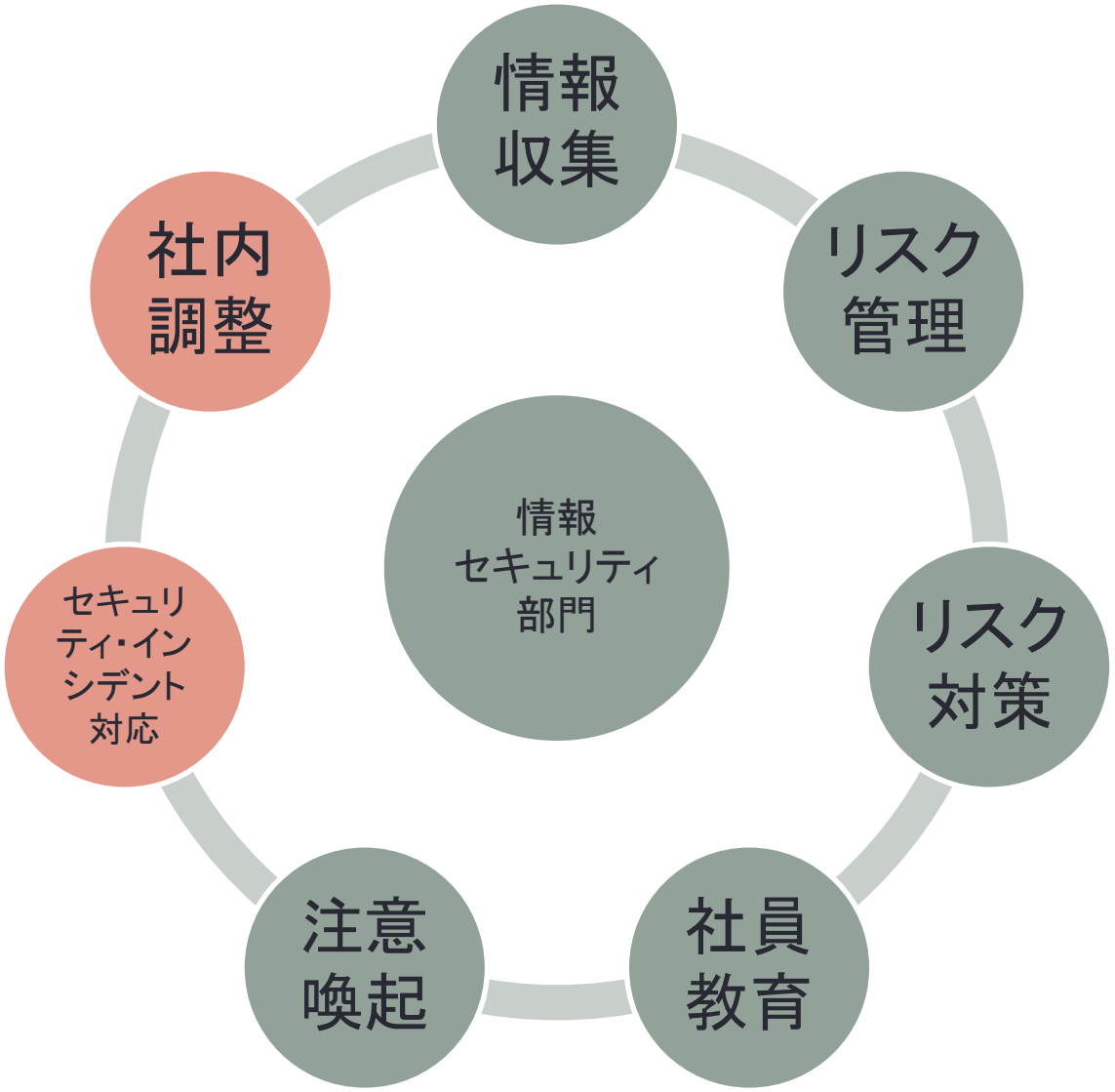
職務の分掌と監督

申請 ＋ 確認 ＝ 承認

承認 ＋ 指示 ＝ 作業

設定 ＋ 分析 ＝ 報告

情報セキュリティ部門の業務範囲



セキュリティ・インシデント対応

- 事象　サイバー攻撃 or 内部不正等・・・・
- 確保　調査対象の確保
- 分析　調査の実施（目的・方法・期間・・・）
- 報告　中間報告、最終報告
- 対応　追加調査、ヒアリング、監視、範囲の確認
- 回復　データの削除、マルウェアの削除

Redline

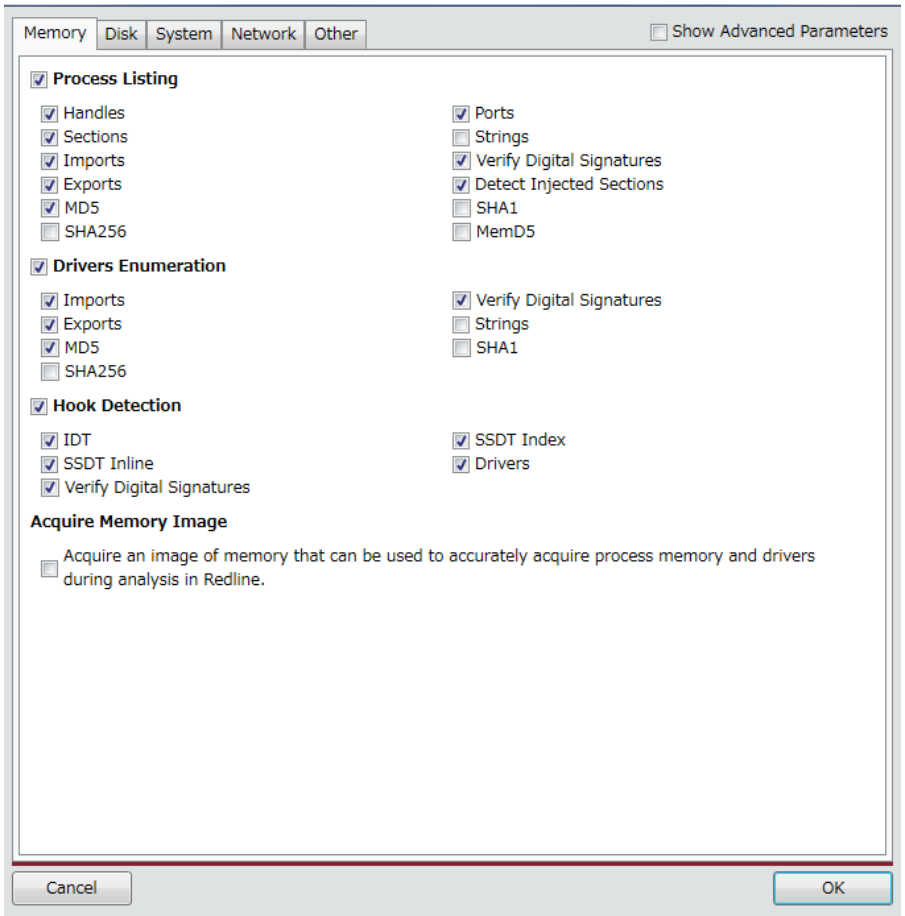
メモリとファイル解析を通して悪意のある活動の兆候ホストを調査を行うツールです。

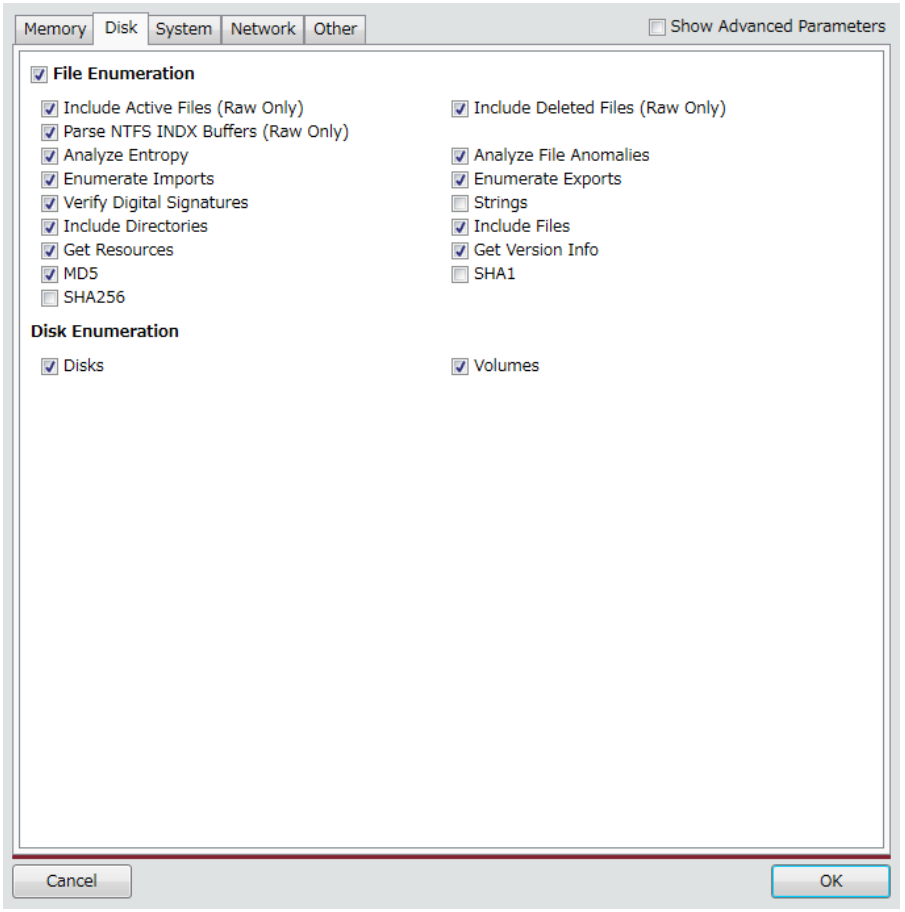
System Requirements

Windows 8 (32-bit and 64-bit versions)
Windows 7 (32-bit and 64-bit versions)
Microsoft Vista (32-bit version)
Windows XP SP2 (32-bit version)
Windows Server 2008 R2 (64-bit version)
Windows Server 2003 SP2 (32-bit versions)
Windows Server 2003 SP2 (64-bit versions)
Windows Server 2000 SP4 (32-bit version)

出所：ファイア・アイ株式会社https://www.mandiant.com/

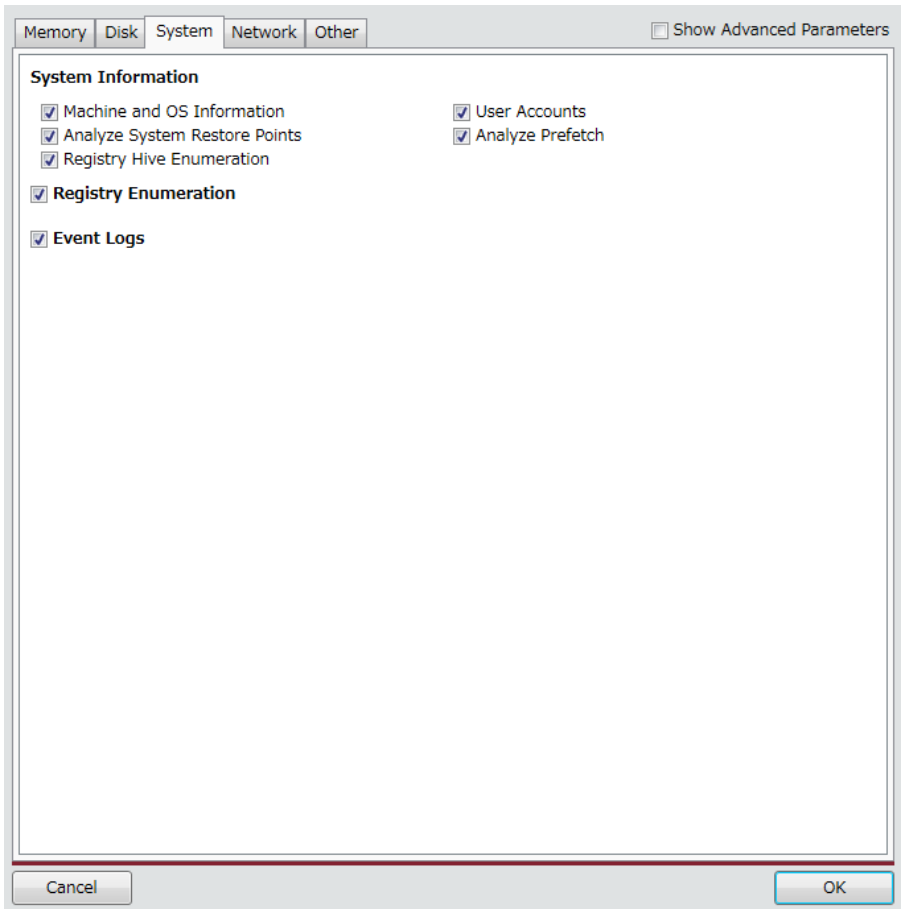
調査項目

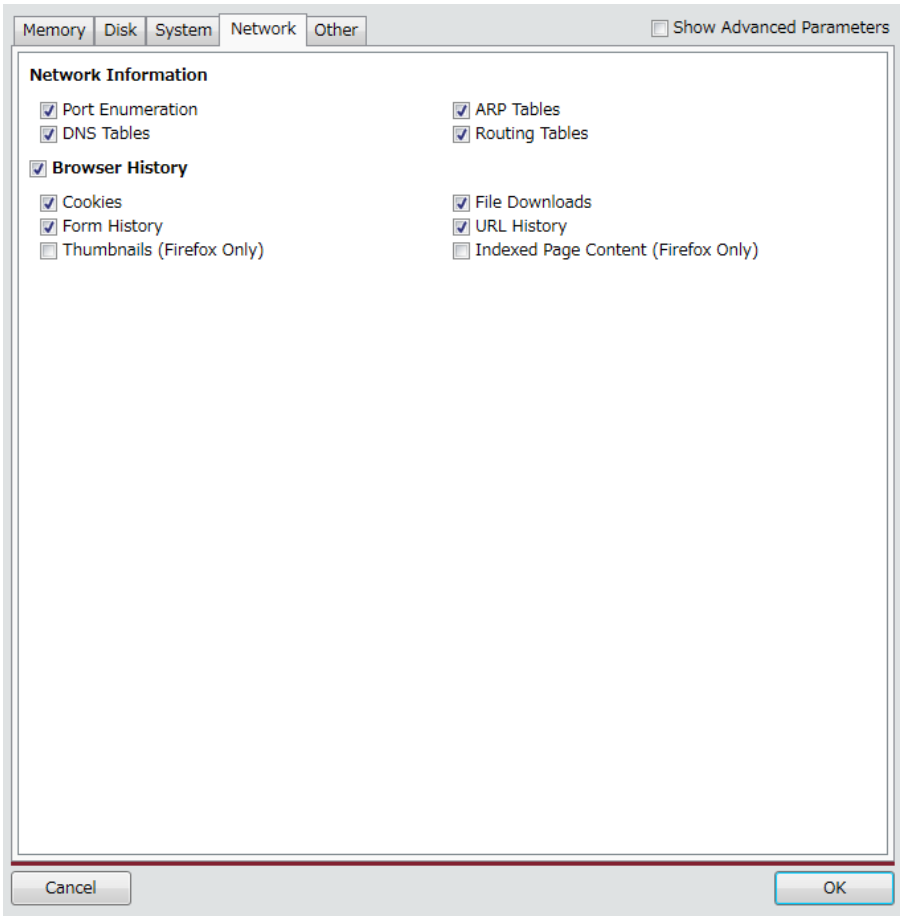




出所：ファイア・アイ株式会社https://www.mandiant.com/

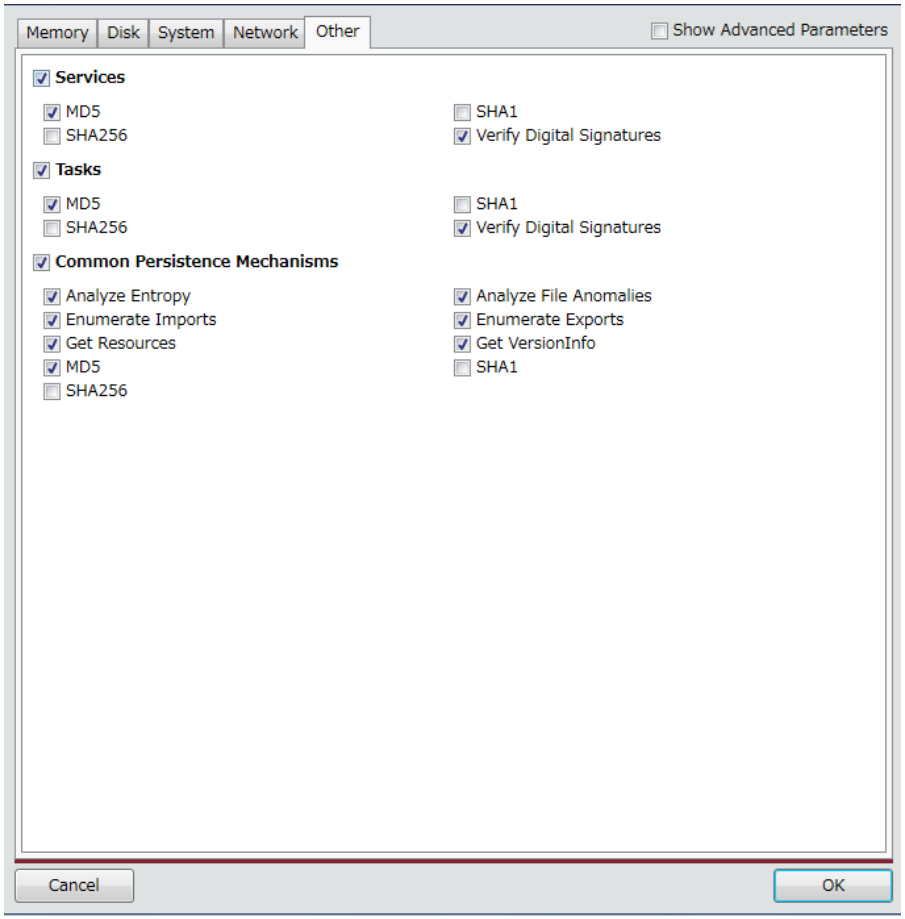
調査項目





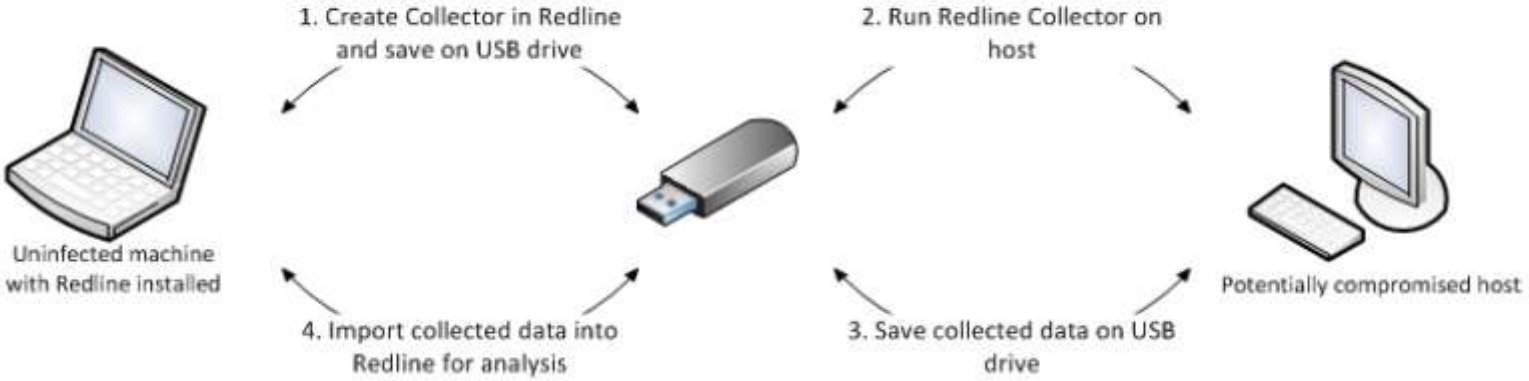
出所：ファイア・アイ株式会社https://www.mandiant.com/

調査項目



出所：ファイア・アイ株式会社https://www.mandiant.com/

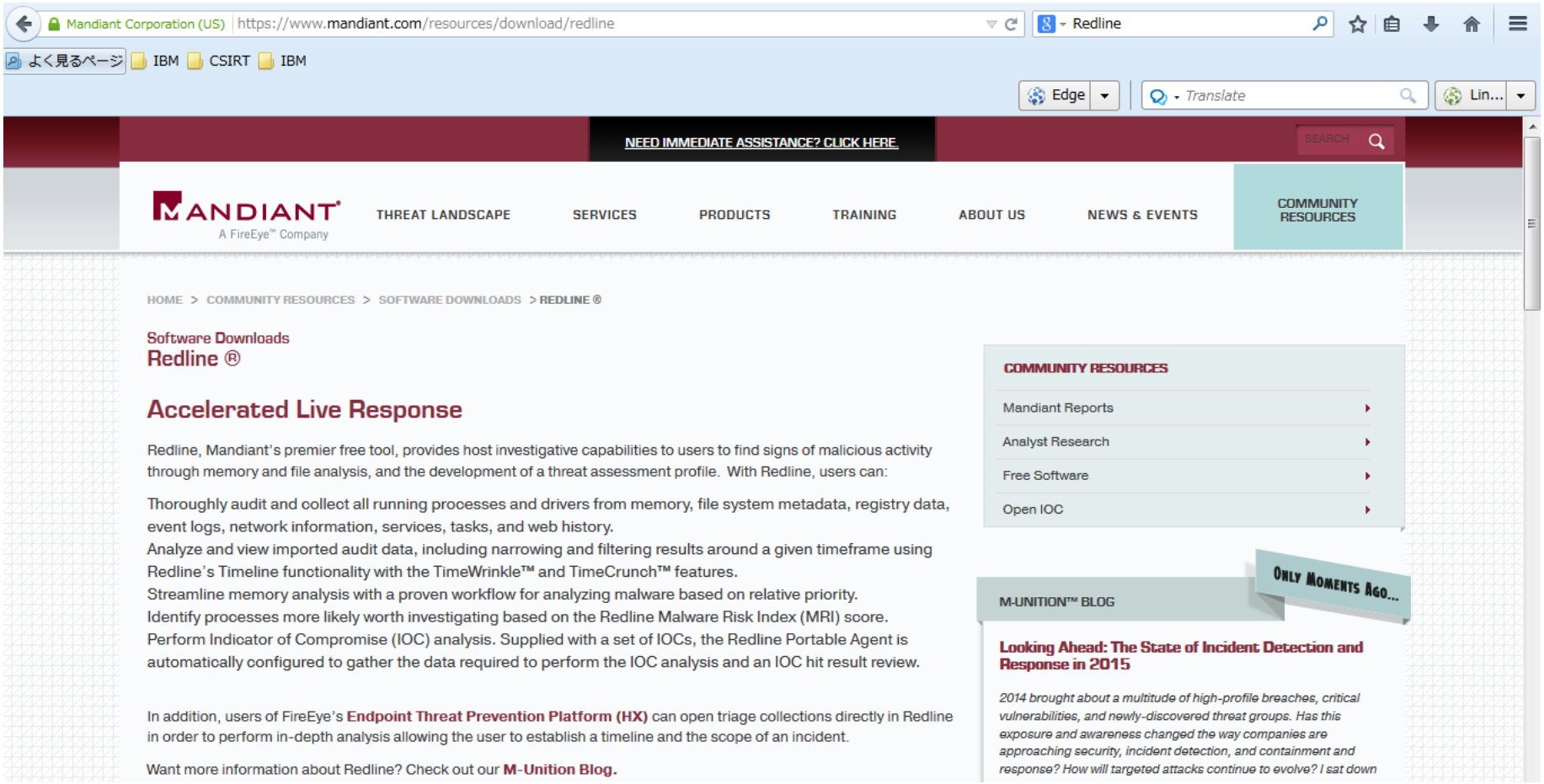
Redlineの利用イメージ



出所：ファイア・アイ株式会社https://www.mandiant.com/

Redlineのダウンロード手順

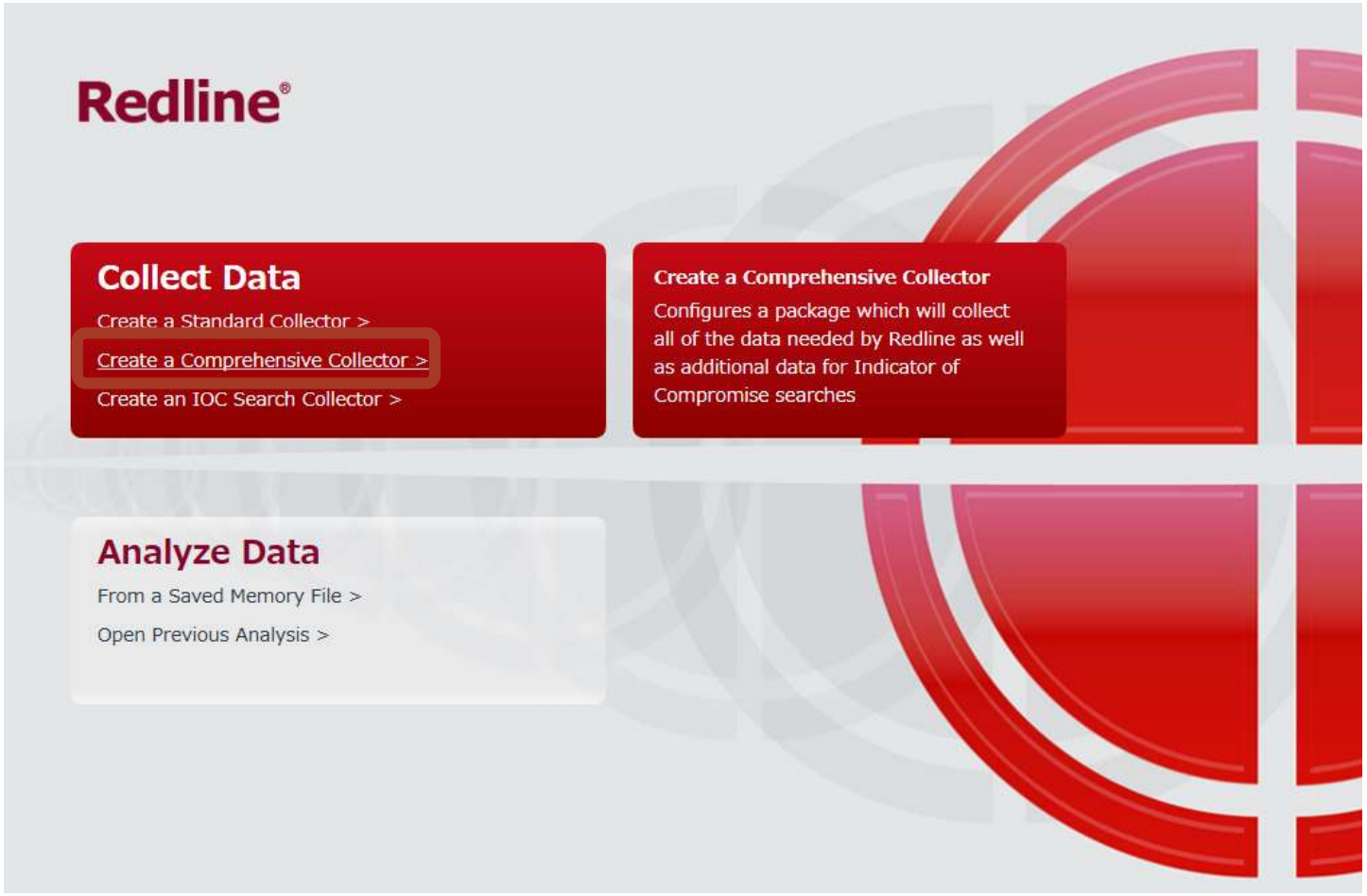
ツールをダウンロードするため、以下のURLにアクセスします。
https://www.mandiant.com/resources/download/redline



出所：ファイア・アイ株式会社https://www.mandiant.com/

①Redline分析モジュールの作成手順

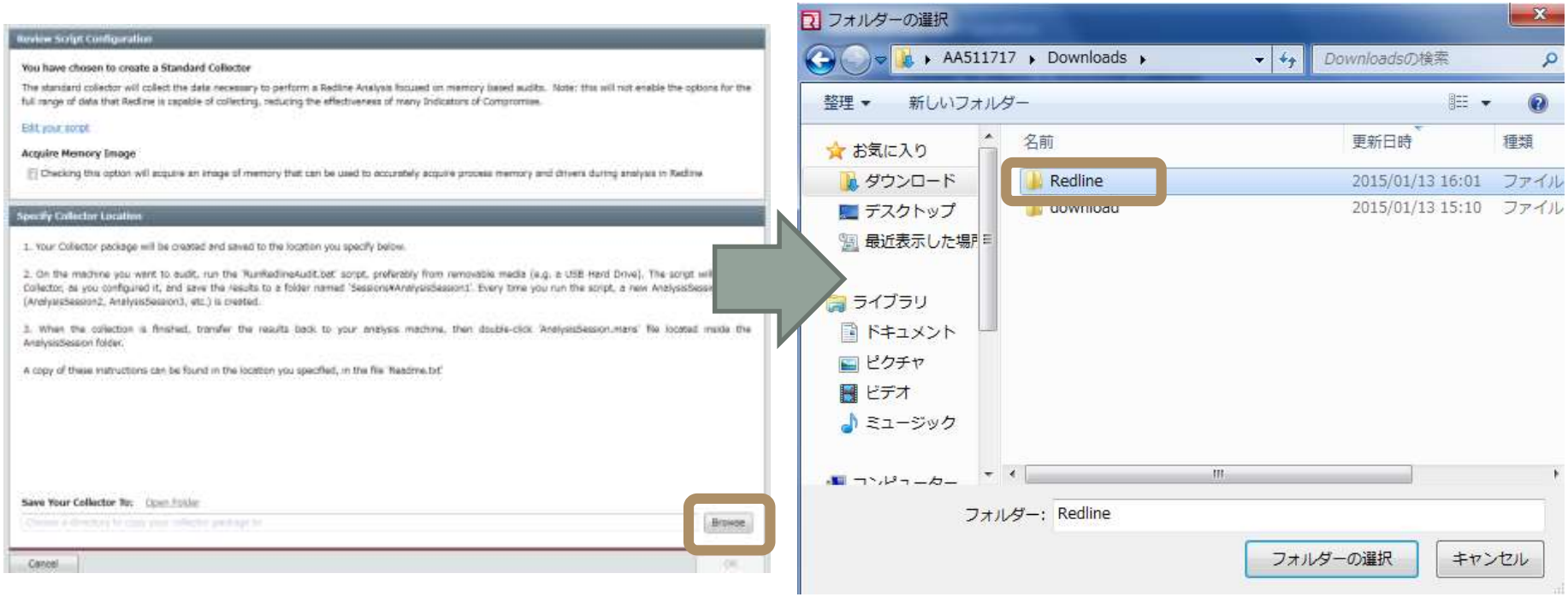
“Create a Comprehensive Collector”は、総合的なデータが収集を行います。



出所：ファイア・アイ株式会社https://www.mandiant.com/

① Redline分析モジュールの作成手順

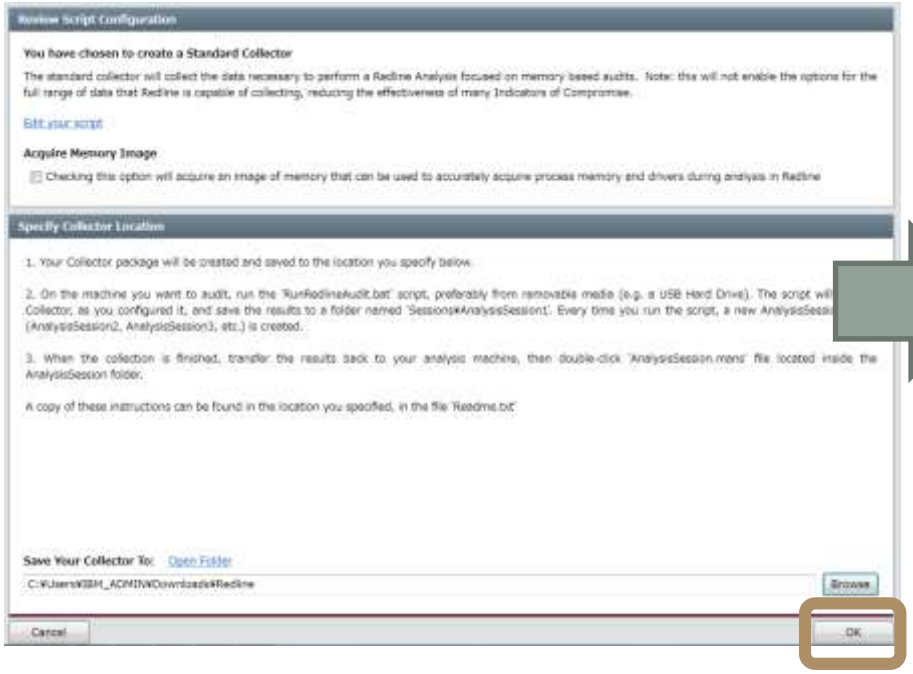
データを収集するためのモジュールを保存するため、新規でフォルダーを作成します。このケースでは、「Redline」というフォルダーを作成しました。モジュールの保存先を指定します。※注：フォルダー名を日本語に設定するとエラーが発生します。



出所：ファイア・アイ株式会社https://www.mandiant.com/

① Redline分析モジュールの作成手順

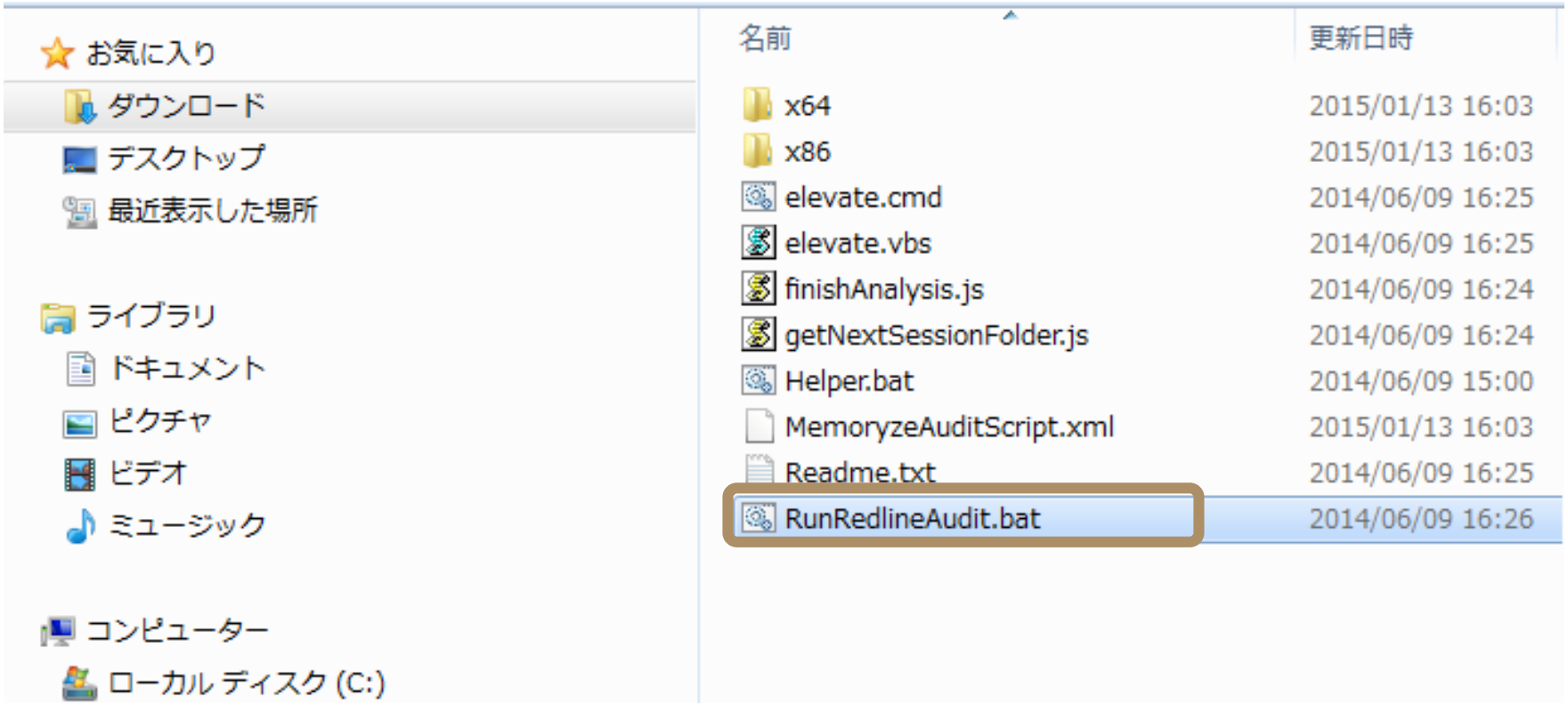
保存先を設定した後は、OKをクリックします。右に表示されたポップアップ画面が表示されるとモジュールが正しく生成されたことを示しています。



出所：ファイア・アイ株式会社https://www.mandiant.com/

②Redline分析モジュールの使用手順

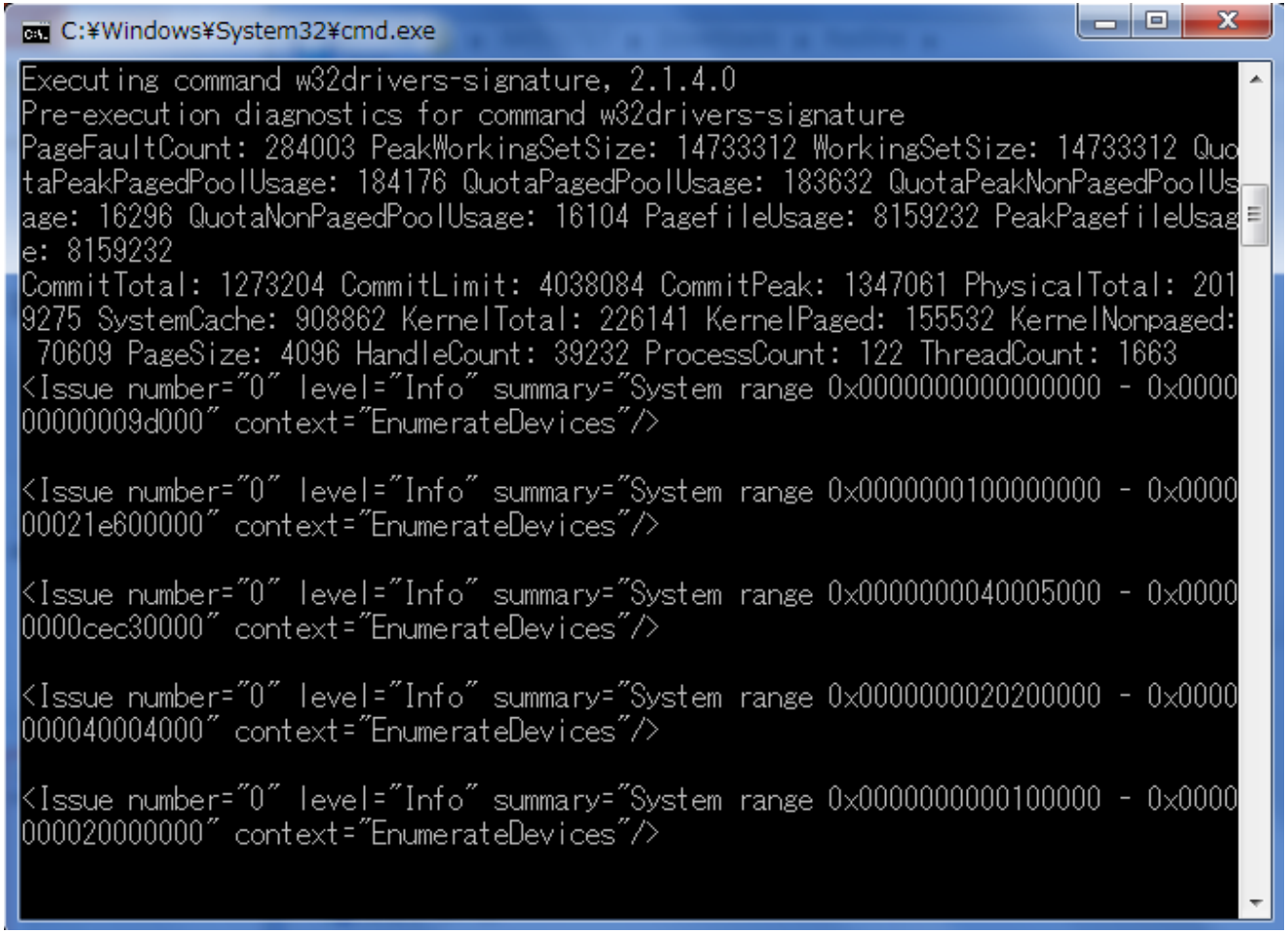
調査対象のPCでモジュールが保存されたフォルダーを開きます。
RunRedlineAudit.batをクリックします。これにより調査データの収集が開始されます。



出所：ファイア・アイ株式会社https://www.mandiant.com/

②Redline分析モジュールの使用手順

データの収集が開始されると図のような画面が起動します。



出所：ファイア・アイ株式会社https://www.mandiant.com/

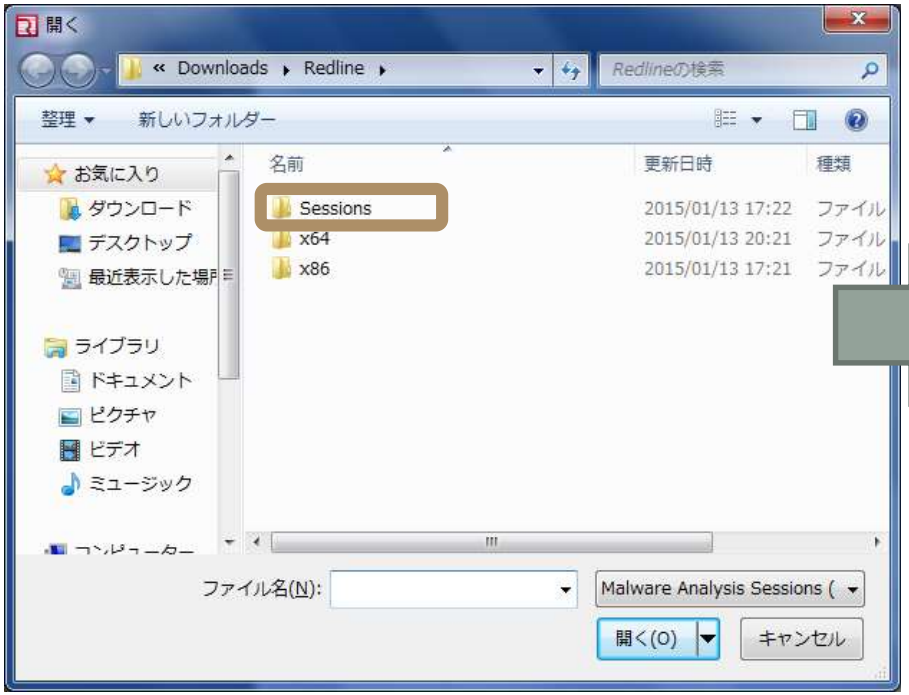
③Redlineによる調査手順

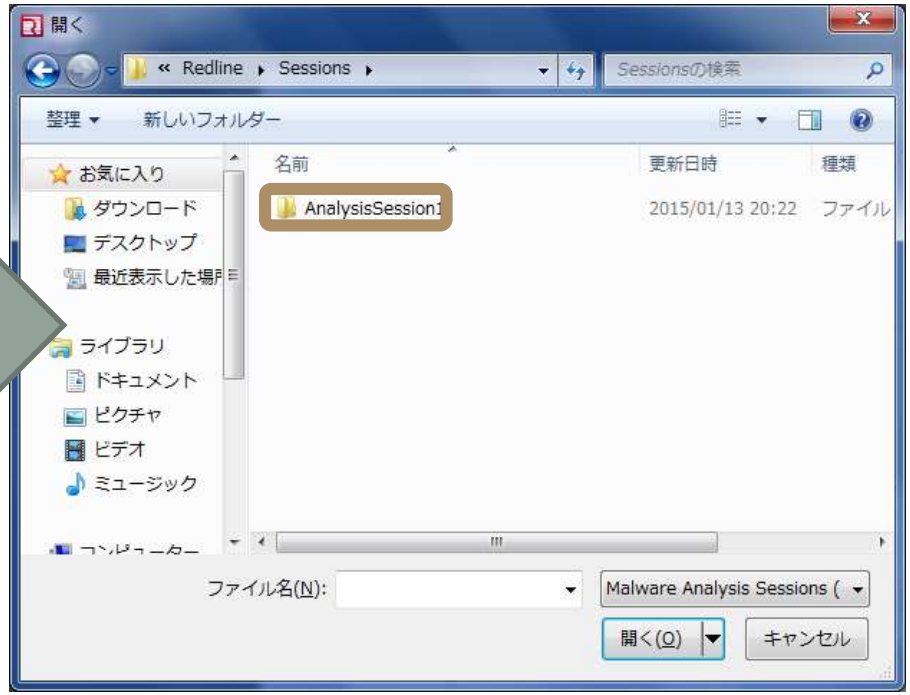
ここからは、Redlineによる調査方法を説明します。まずは、Analyze DataからOpen Previous Analysisをクリックしてください。

出所：ファイア・アイ株式会社https://www.mandiant.com/

③Redlineによる調査手順

情報を収集するためのモジュールが保存されている場所に移動します。
そこから[Sessions]→[AnalysisSession]を選択します。

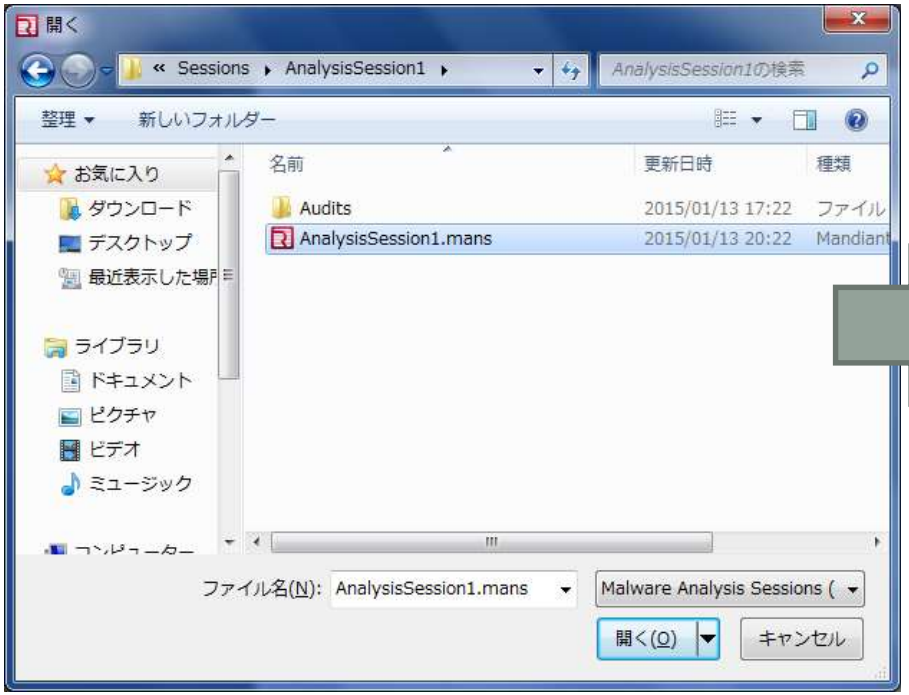




出所：ファイア・アイ株式会社https://www.mandiant.com/

③Redlineによる調査手順

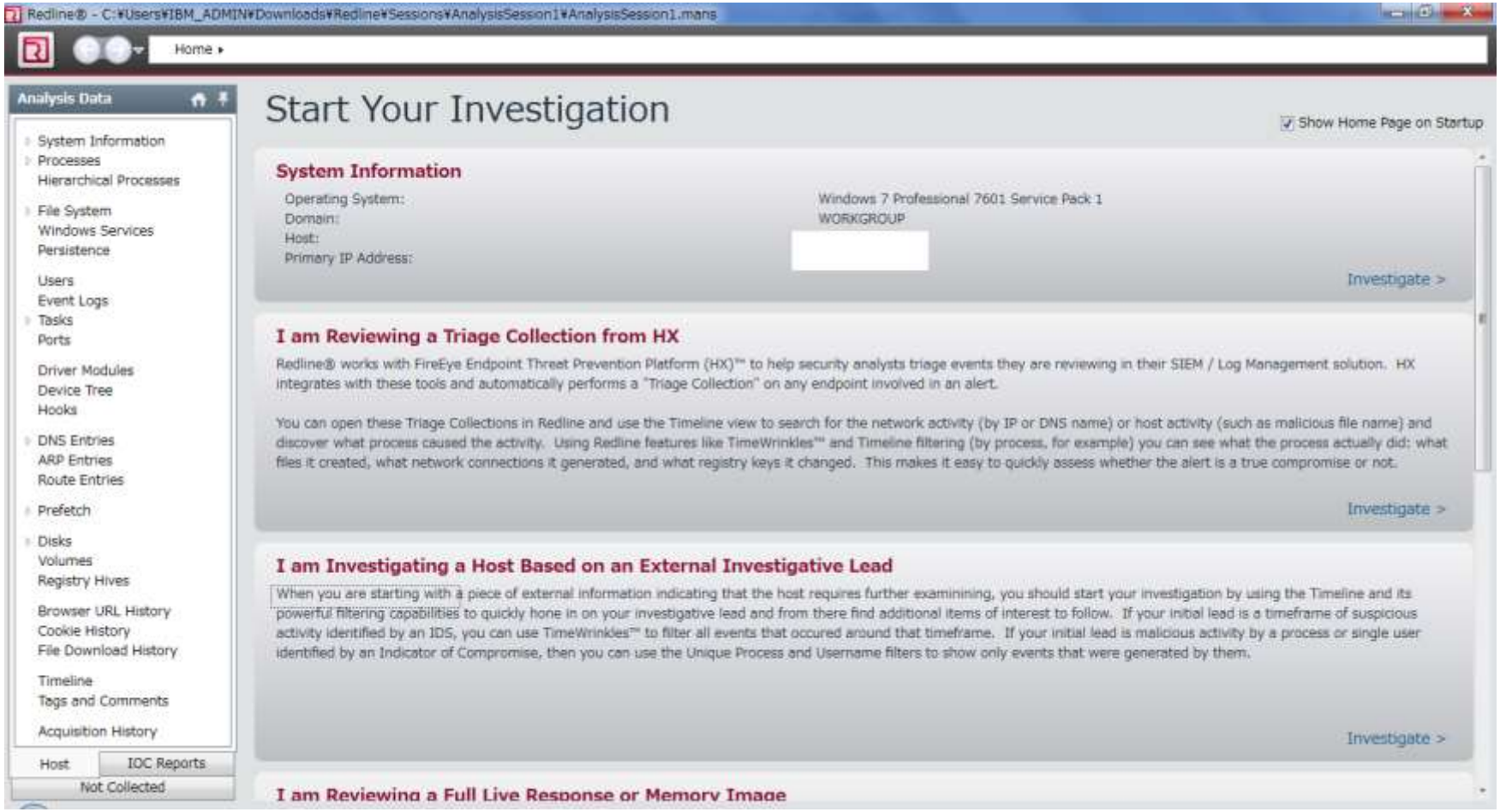
次に拡張子がmansのファイルを選択します。
今回のケースでは、[AnalysisSession1.mans]を選択するとRedlineにデータが読み込まれます。読み込みには、数十分掛かります。



出所：ファイア・アイ株式会社https://www.mandiant.com/

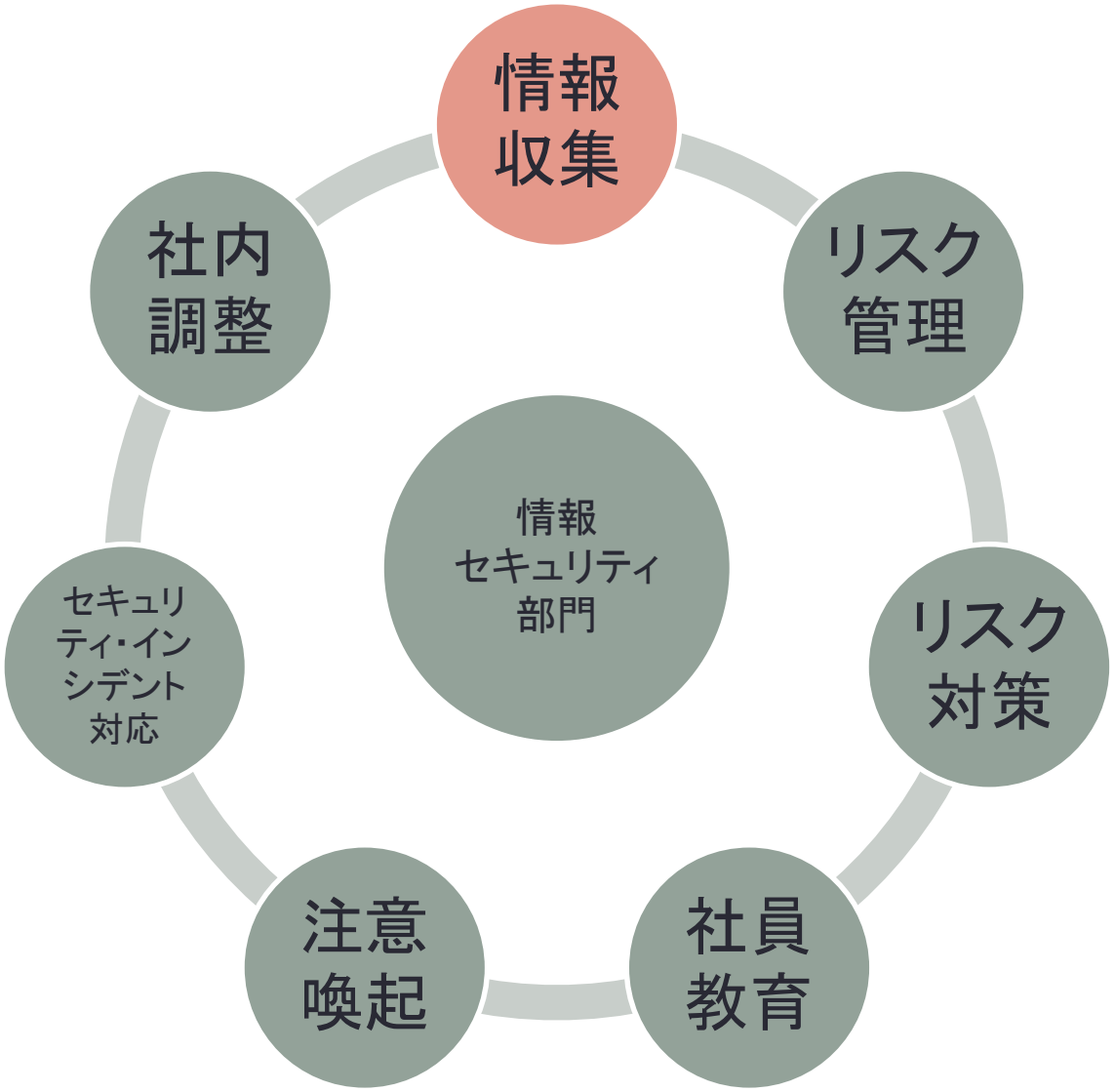
③Redlineによる調査手順

データの読み込みが完了すると、以下のような画面が表示されます。

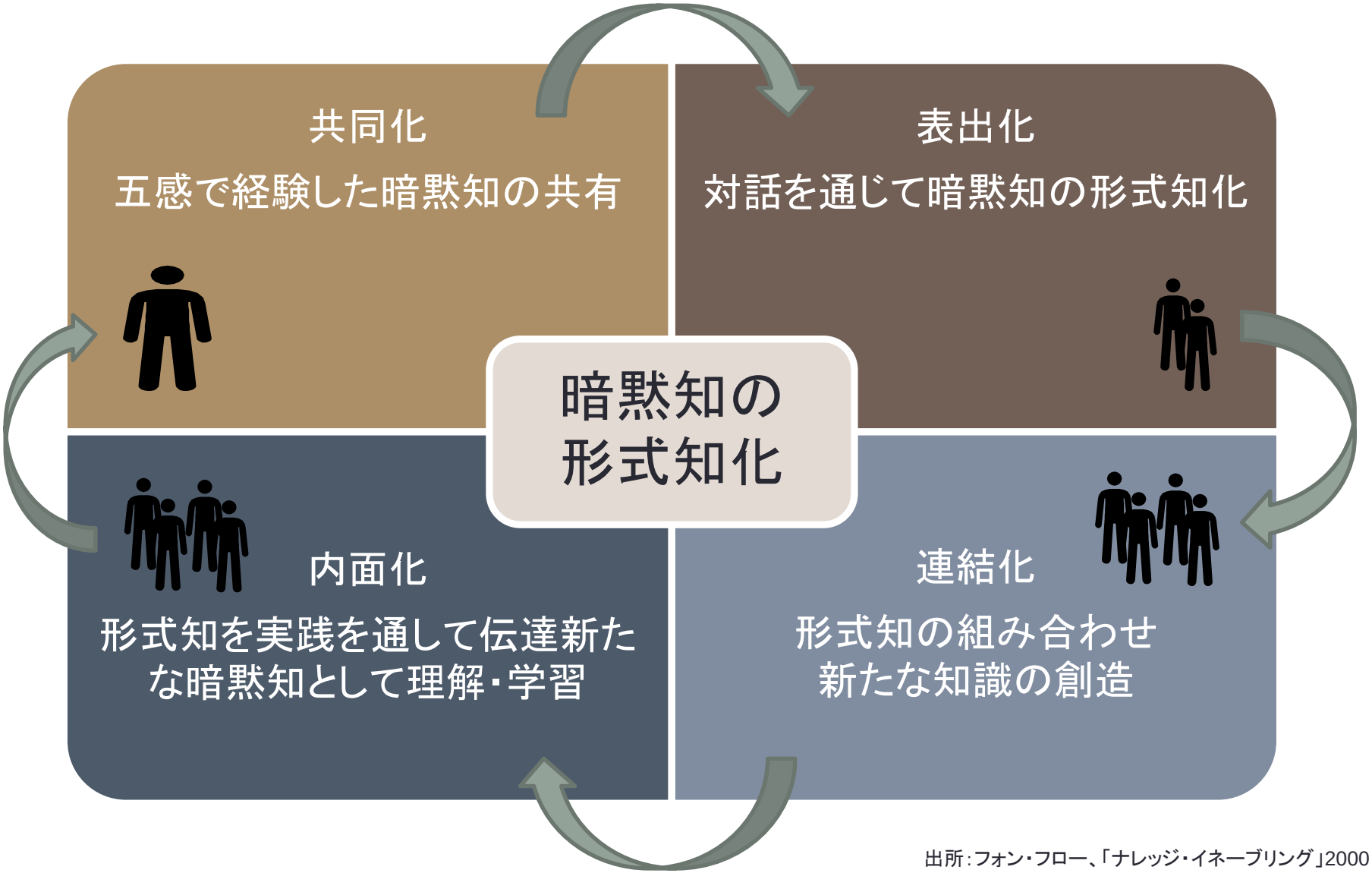


出所：ファイア・アイ株式会社https://www.mandiant.com/

情報セキュリティ部門の業務範囲



知識創造



出所：フォン・フロー、「ナレッジ・イネーブリング」2000

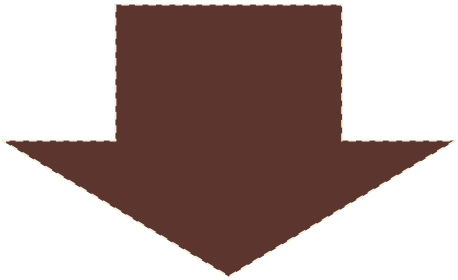
日本シーサーと協議会 インシデント事例分析WG

◆活動内容：

複数の企業でインシデント事例を分析する事により『効率的な対応』や『効果的な対策』が導き出せることを目的とし、社内および社外への連絡方法、社内体制(法務、営業など)、効果的な再発防止策に関する分析を行う。

野獣の原則（P.F.ドラッカーの社会的責任）

ライオンが檻から逃げたら責任は飼い主にある。
過失により檻が開いたか、地震でカギが外れたかは関係ない。
ライオンが凶暴であることは避けられない。



企業は故意・過失を問わず
広範な責任を負っている

出所：サイバーセキュリティ　第5章　浅沼宏和氏株式会社TMAコンサルティング 代表取締役/浅沼総合会計事務所 所長（NTT出版）

ワークショップ、セッション、および資料は、発表者によって準備され、それぞれ独自の見解を反映したものです。それらは情報提供の目的のみで提供されており、いかなる参加者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本講演資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本講演資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、発表者は責任を負わないものとします。 本講演資料に含まれている内容は、いかなる保証または表明を引きだすことを意図したものでも、またそのような結果を生むものでもありません。

本講演資料で製品、プログラム、またはサービスに言及していても、営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本講演資料に含まれている内容は、参加者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。 ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。