

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

■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



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。



矢野経済研究所<http://japan.zdnet.com/article/35056740/>

サイバー攻撃

高度な
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

陳腐な
手法

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

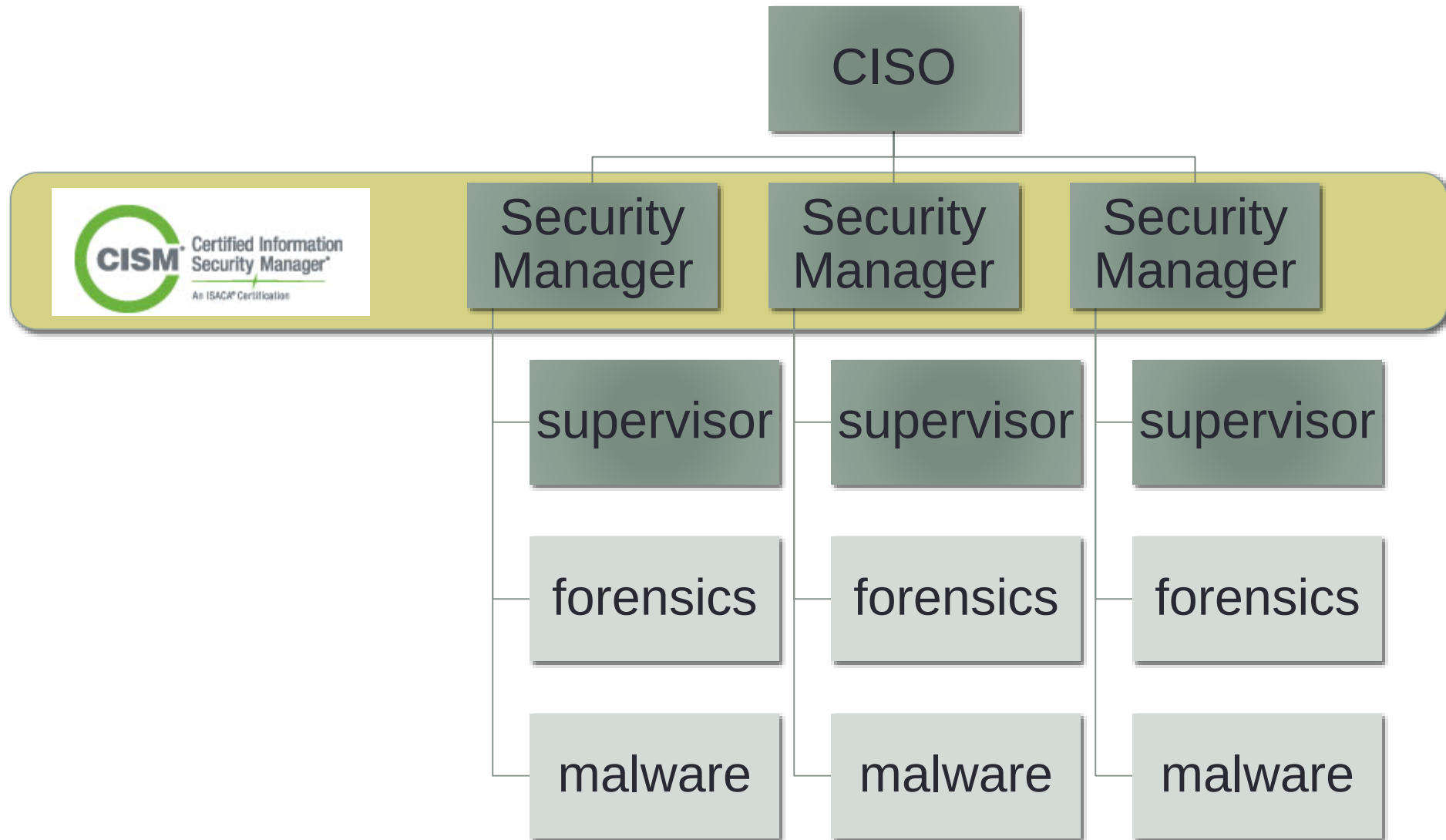
攻撃対象が広範

攻撃対象が限定的

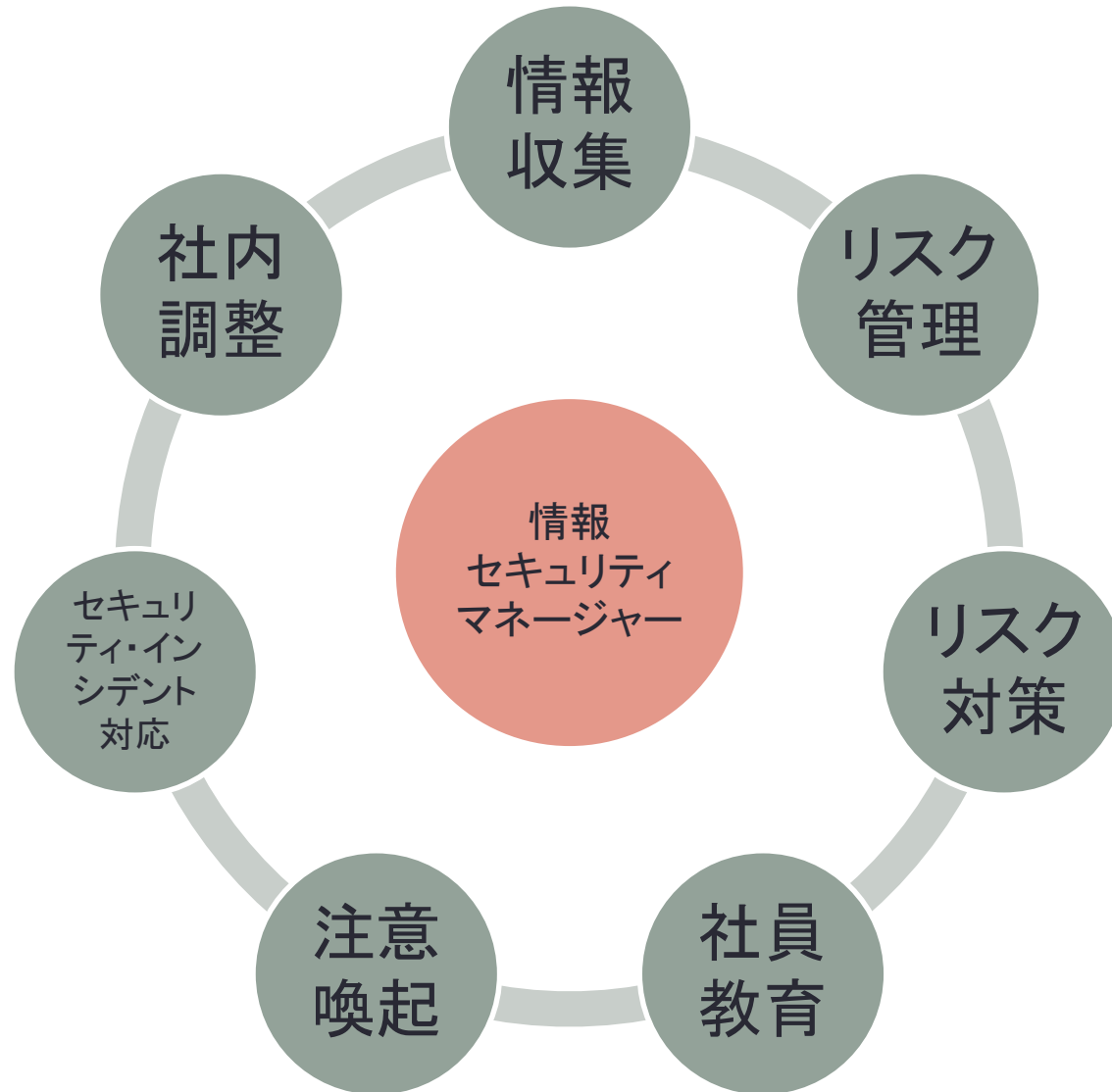
内部不正

	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

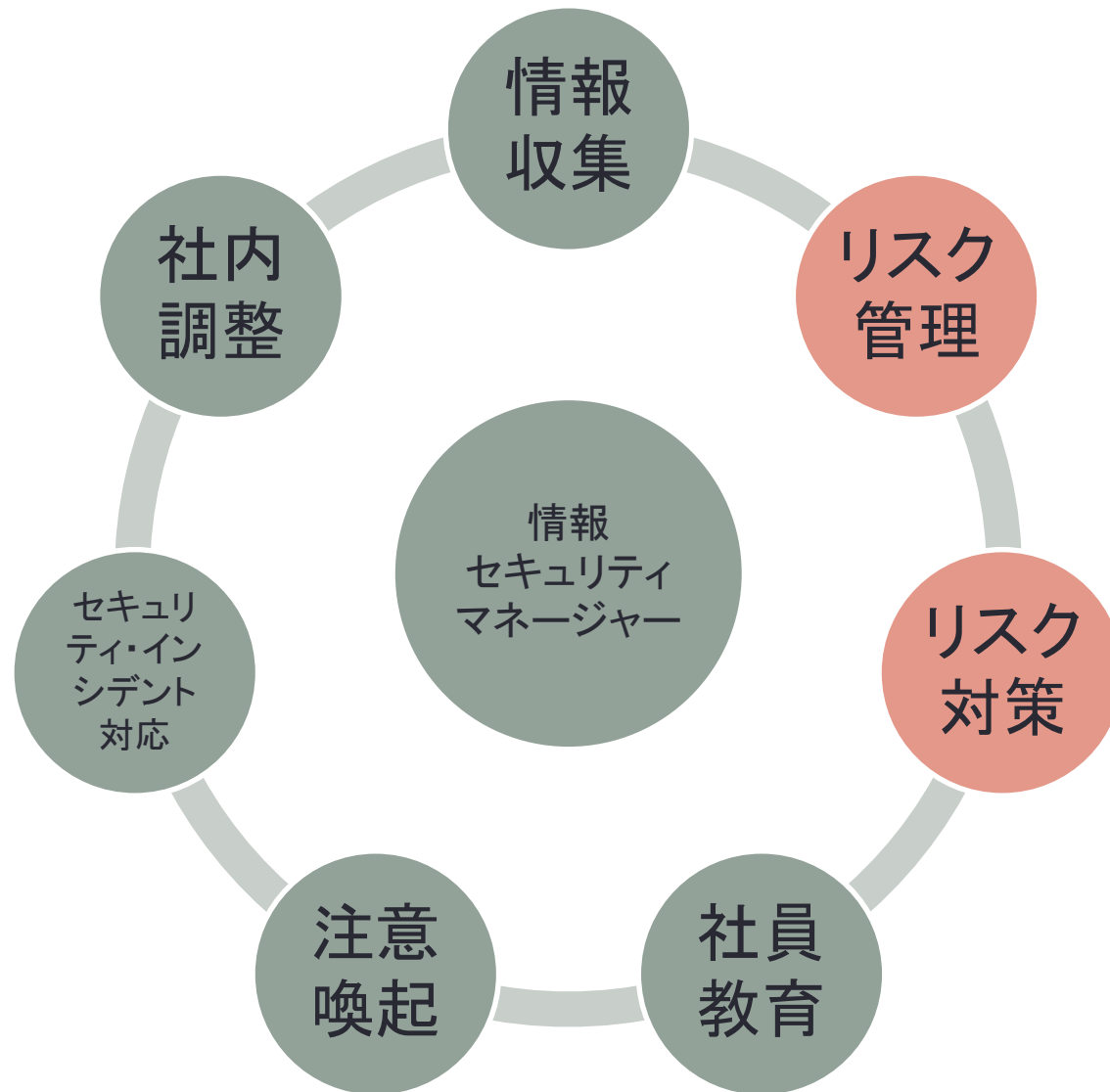
運用体制



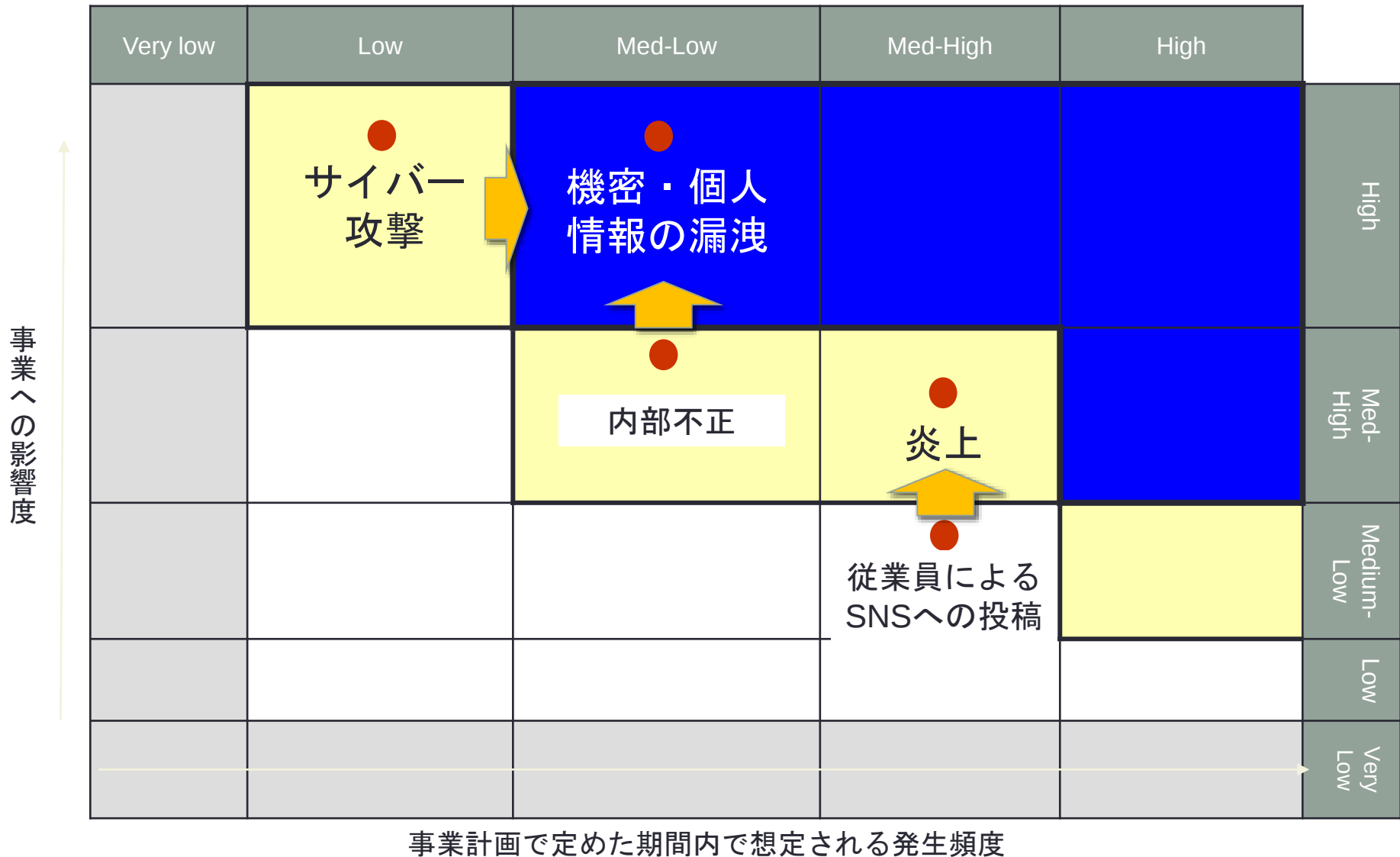
情報セキュリティ部門の業務範囲



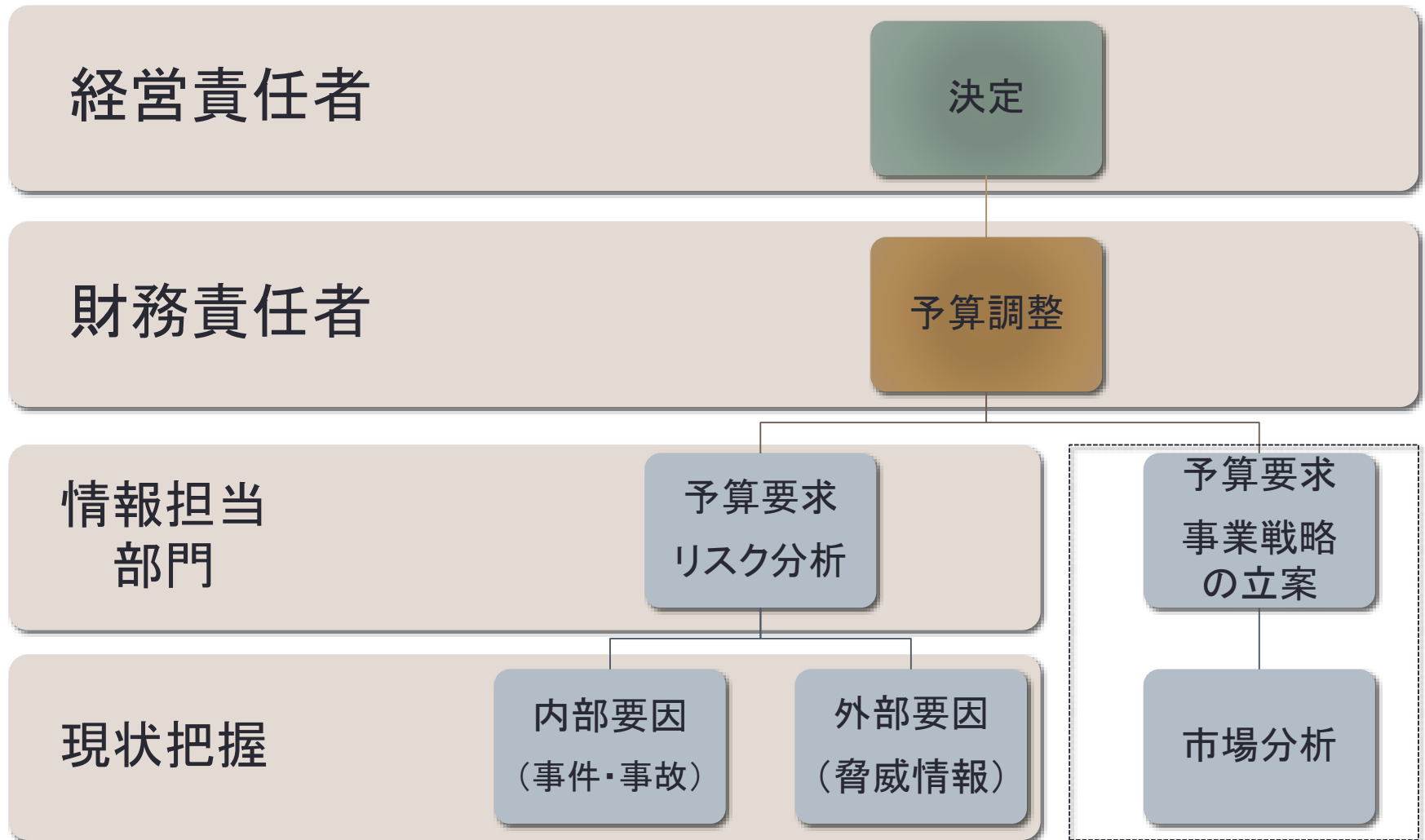
情報セキュリティ部門の業務範囲



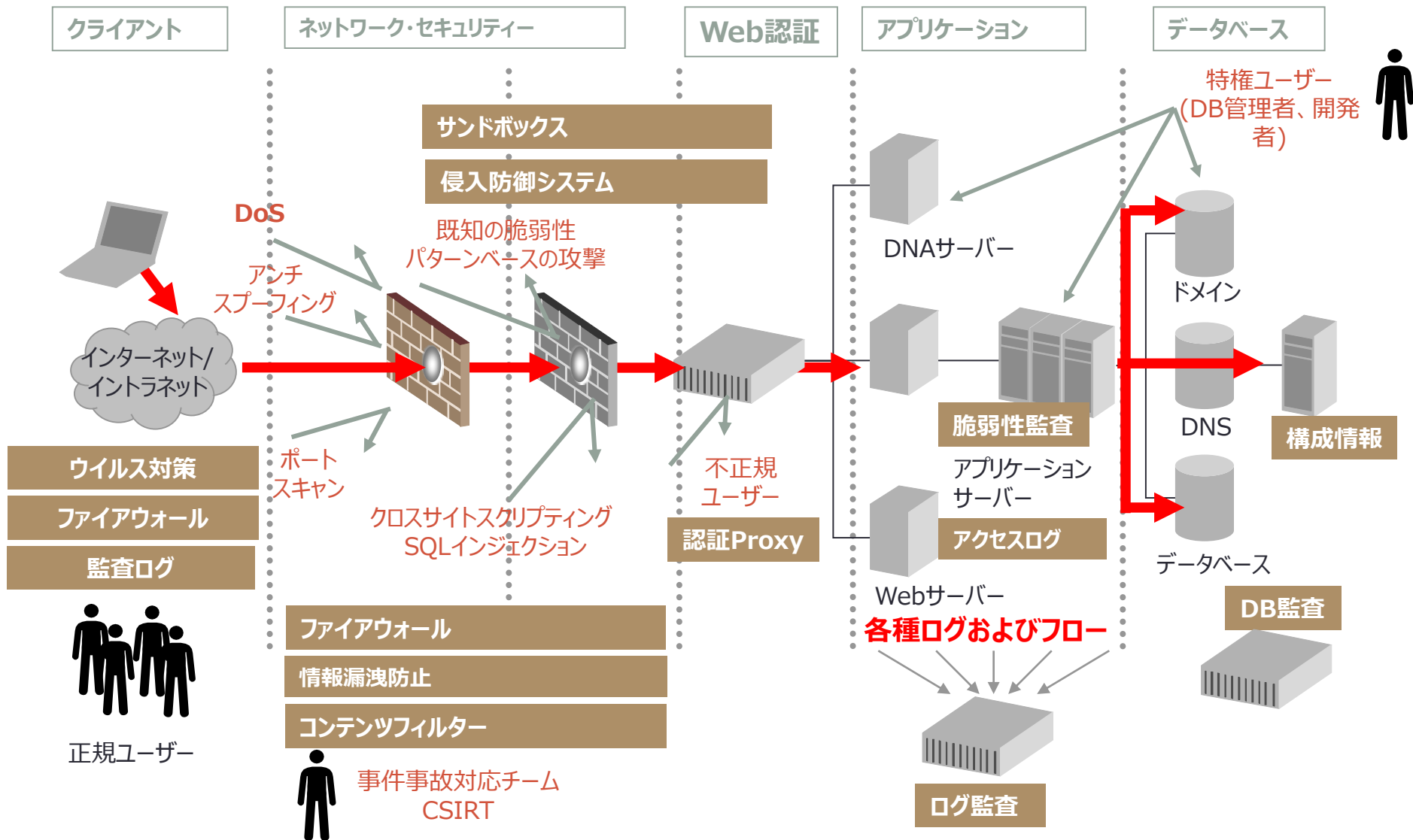
リスクの分析



予算化



対策の検討



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

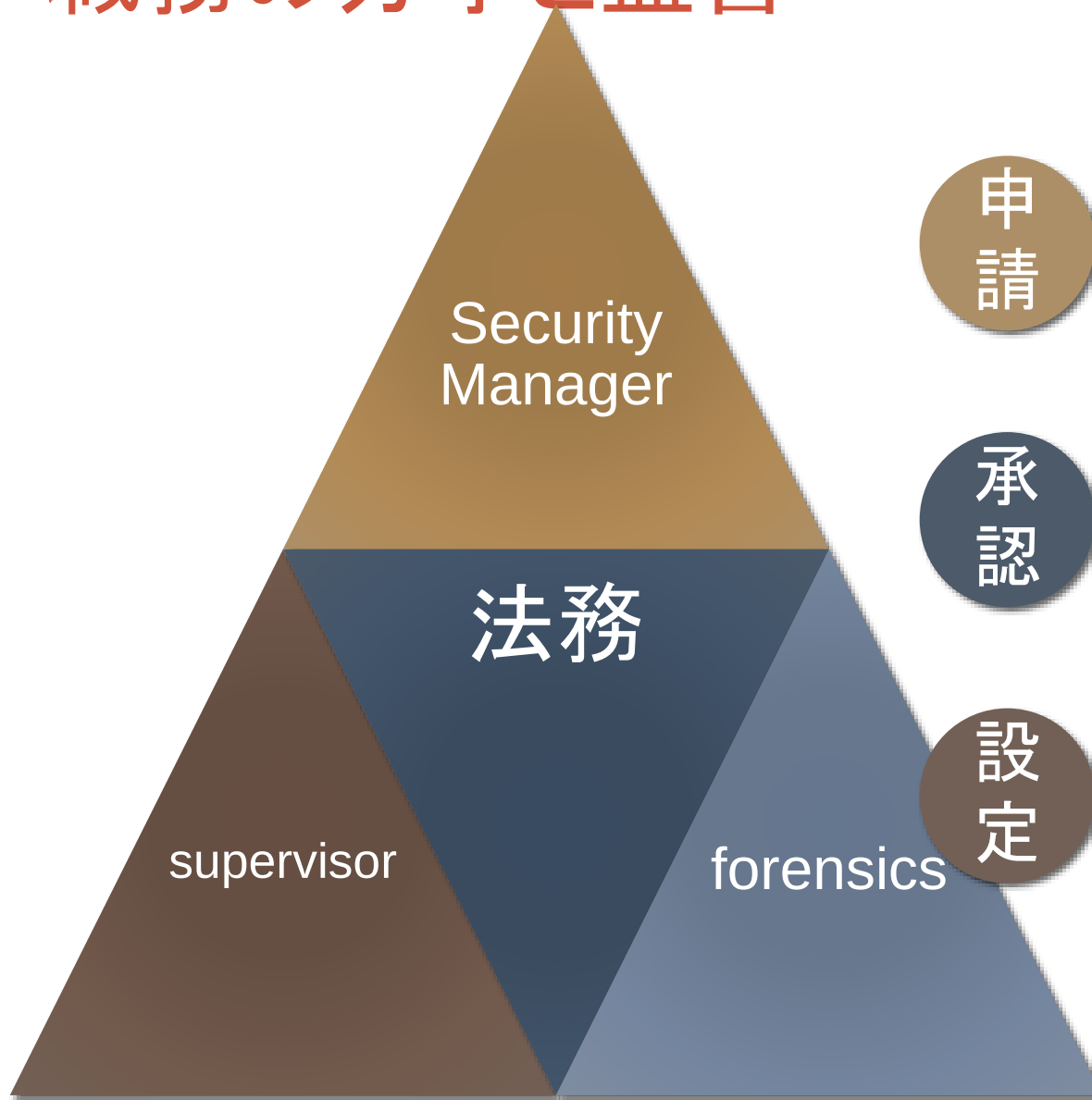
IV

- ・ 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

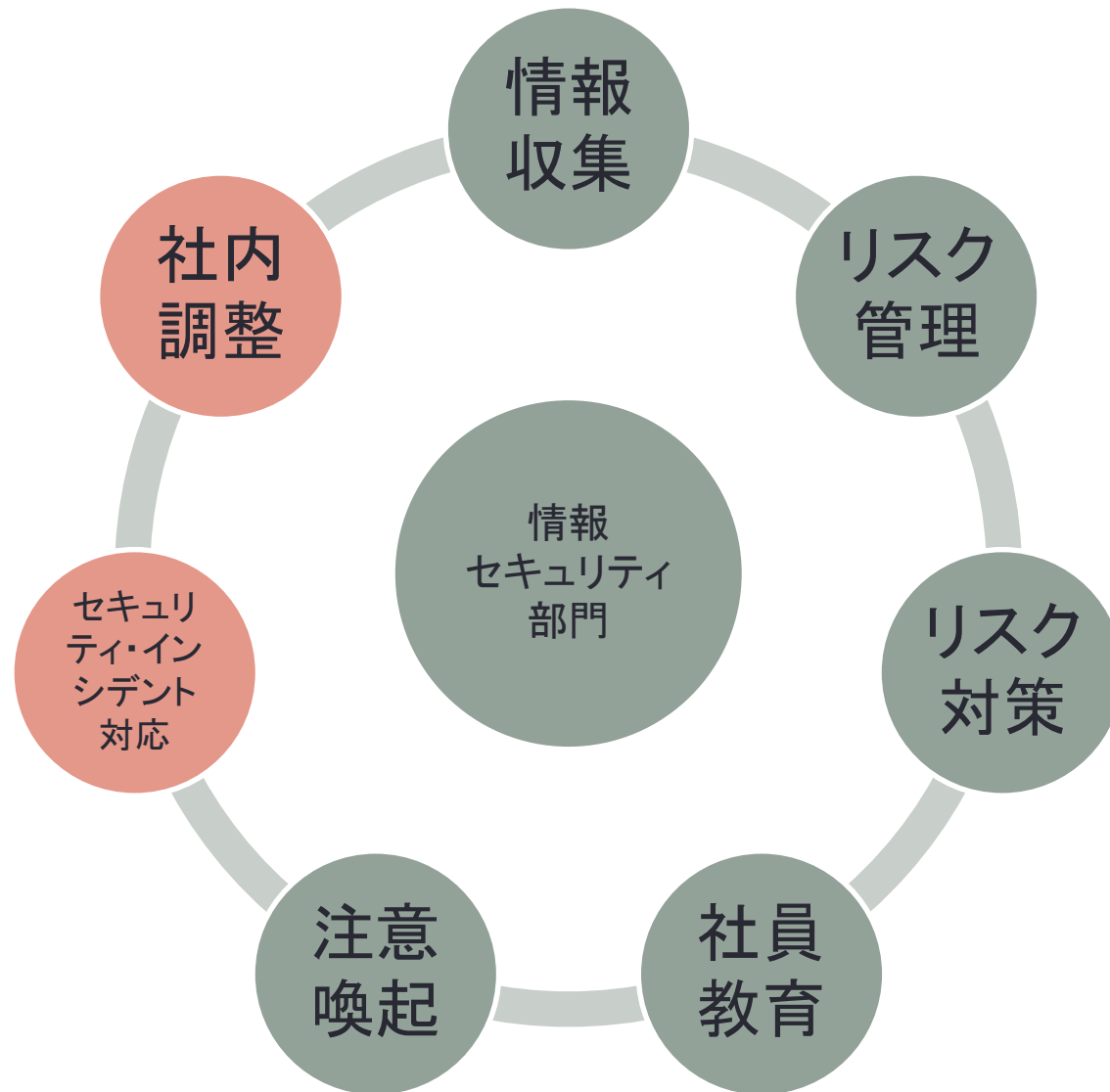
V

- ・ 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

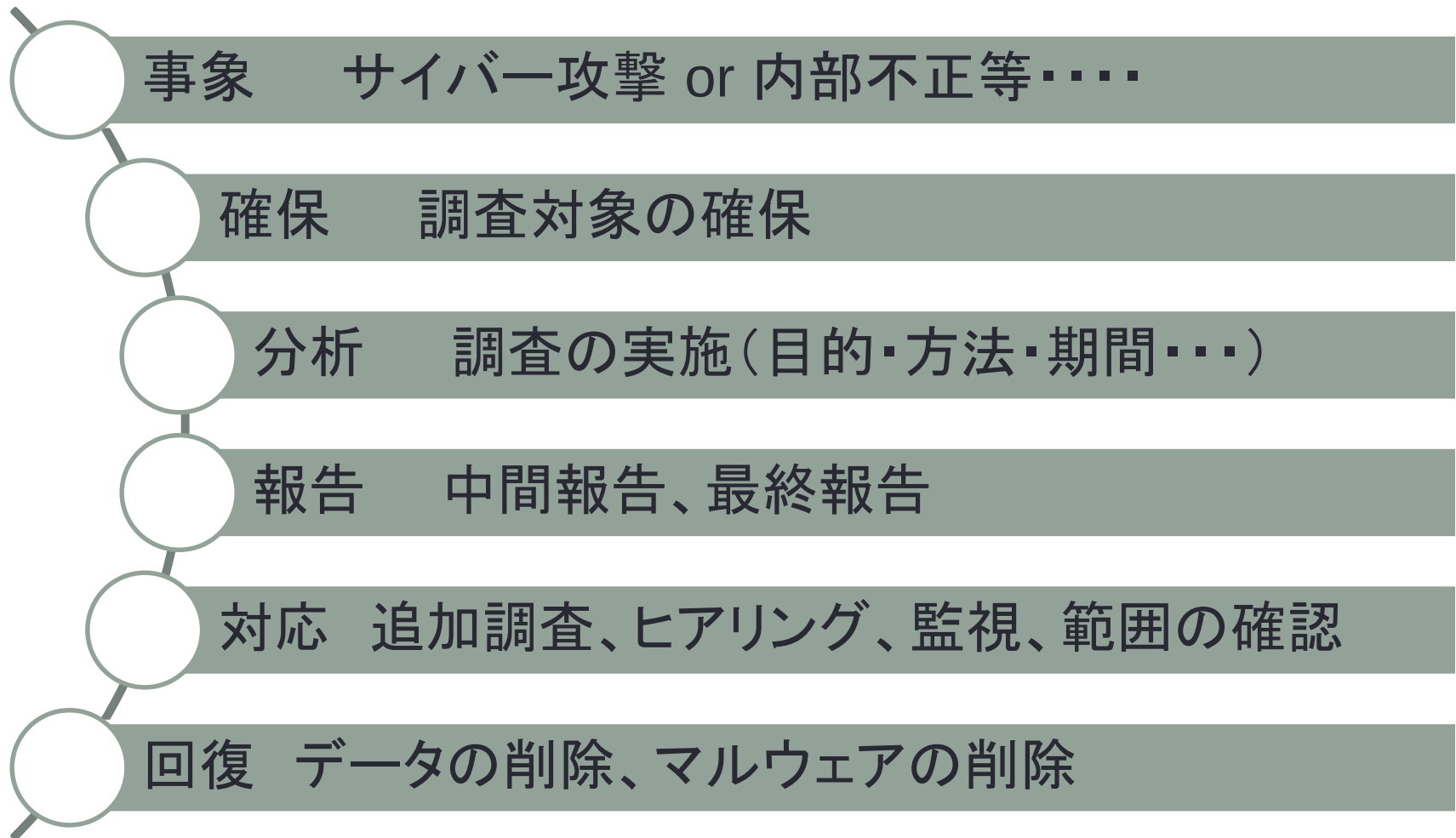
職務の分掌と監督



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



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)

調査項目

Memory Disk System Network Other ☐ Show Advanced Parameters

☒ **Process Listing**

- ☒ Handles
- ☒ Sections
- ☒ Imports
- ☒ Exports
- ☒ MD5
- ☐ SHA256

☒ **Drivers Enumeration**

- ☒ Imports
- ☒ Exports
- ☒ MD5
- ☐ SHA256

☒ **Hook Detection**

- ☒ IDT
- ☒ SSDT Inline
- ☒ Verify Digital Signatures

Acquire Memory Image

☐ Acquire an image of memory that can be used to accurately acquire process memory and drivers during analysis in Redline.

Cancel OK

Memory Disk System Network Other ☐ Show Advanced Parameters

☒ **File Enumeration**

- ☒ Include Active Files (Raw Only)
- ☒ Parse NTFS INDEX Buffers (Raw Only)
- ☒ Analyze Entropy
- ☒ Enumerate Imports
- ☒ Verify Digital Signatures
- ☒ Include Directories
- ☒ Get Resources
- ☒ MD5
- ☐ SHA256

☒ Include Deleted Files (Raw Only)

☒ Analyze File Anomalies

☒ Enumerate Exports

☐ Strings

☒ Include Files

☒ Get Version Info

☐ SHA1

Disk Enumeration

- ☒ Disks
- ☒ Volumes

Cancel OK

調査項目

Memory Disk System Network Other ☐ Show Advanced Parameters

System Information

- ☒ Machine and OS Information
- ☒ Analyze System Restore Points
- ☒ Registry Hive Enumeration
- ☒ Registry Enumeration
- ☒ Event Logs
- ☒ User Accounts
- ☒ Analyze Prefetch

Cancel OK

Memory Disk System Network Other ☐ Show Advanced Parameters

Network Information

- ☒ Port Enumeration
- ☒ DNS Tables
- ☒ Browser History
 - ☒ Cookies
 - ☒ Form History
 - ☐ Thumbnails (Firefox Only)
- ☒ ARP Tables
- ☒ Routing Tables
- ☒ File Downloads
- ☒ URL History
- ☐ Indexed Page Content (Firefox Only)

Cancel OK

調査項目

The screenshot shows a software window with a tabbed interface. The 'Other' tab is selected, displaying a list of investigation items organized into three sections: Services, Tasks, and Common Persistence Mechanisms. Each section contains several checkboxes, some of which are checked. A 'Show Advanced Parameters' checkbox is located at the top right of the window. The bottom of the window features 'Cancel' and 'OK' buttons.

Memory Disk System Network Other ☐ Show Advanced Parameters

☒ **Services**

- ☒ MD5
- ☐ SHA256
- ☐ SHA1
- ☒ Verify Digital Signatures

☒ **Tasks**

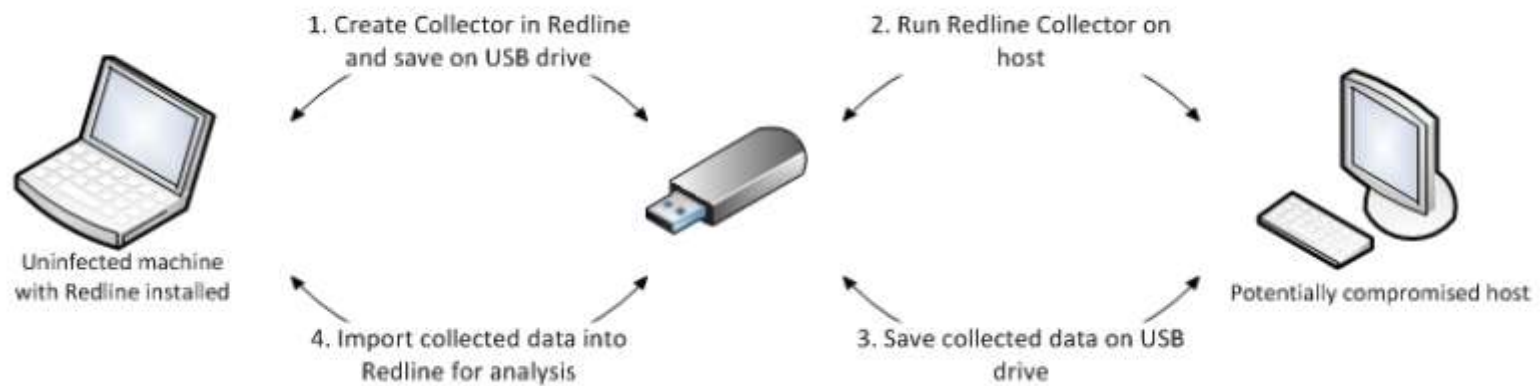
- ☒ MD5
- ☐ SHA256
- ☐ SHA1
- ☒ Verify Digital Signatures

☒ **Common Persistence Mechanisms**

- ☒ Analyze Entropy
- ☒ Enumerate Imports
- ☒ Get Resources
- ☒ MD5
- ☐ SHA256
- ☒ Analyze File Anomalies
- ☒ Enumerate Exports
- ☒ Get VersionInfo
- ☐ SHA1

Cancel OK

Redlineの利用イメージ



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>

Mandiant Corporation (US) | <https://www.mandiant.com/resources/download/redline>

よく見るページ IBM CSIRT IBM

Edge Translate Lin...

NEED IMMEDIATE ASSISTANCE? CLICK HERE

SEARCH

MANDIANT
A FireEye™ Company

THREAT LANDSCAPE SERVICES PRODUCTS TRAINING ABOUT US NEWS & EVENTS COMMUNITY RESOURCES

HOME > COMMUNITY RESOURCES > SOFTWARE DOWNLOADS > REDLINE ®

Software Downloads
Redline ®

Accelerated Live Response

Redline, Mandiant's premier free tool, provides host investigative capabilities to users to find signs of malicious activity through memory and file analysis, and the development of a threat assessment profile. With Redline, users can:

Thoroughly audit and collect all running processes and drivers from memory, file system metadata, registry data, event logs, network information, services, tasks, and web history.

Analyze and view imported audit data, including narrowing and filtering results around a given timeframe using Redline's Timeline functionality with the TimeWrinkle™ and TimeCrunch™ features.

Streamline memory analysis with a proven workflow for analyzing malware based on relative priority.

Identify processes more likely worth investigating based on the Redline Malware Risk Index (MRI) score.

Perform Indicator of Compromise (IOC) analysis. Supplied with a set of IOCs, the Redline Portable Agent is automatically configured to gather the data required to perform the IOC analysis and an IOC hit result review.

In addition, users of FireEye's **Endpoint Threat Prevention Platform (HX)** can open triage collections directly in Redline in order to perform in-depth analysis allowing the user to establish a timeline and the scope of an incident.

Want more information about Redline? Check out our **M-Unition Blog**.

COMMUNITY RESOURCES

- Mandiant Reports
- Analyst Research
- Free Software
- Open IOC

M-UNITION™ BLOG

ONLY MOMENTS AGO...

Looking Ahead: The State of Incident Detection and Response in 2015

2014 brought about a multitude of high-profile breaches, critical vulnerabilities, and newly-discovered threat groups. Has this exposure and awareness changed the way companies are approaching security, incident detection, and containment and response? How will targeted attacks continue to evolve? I sat down

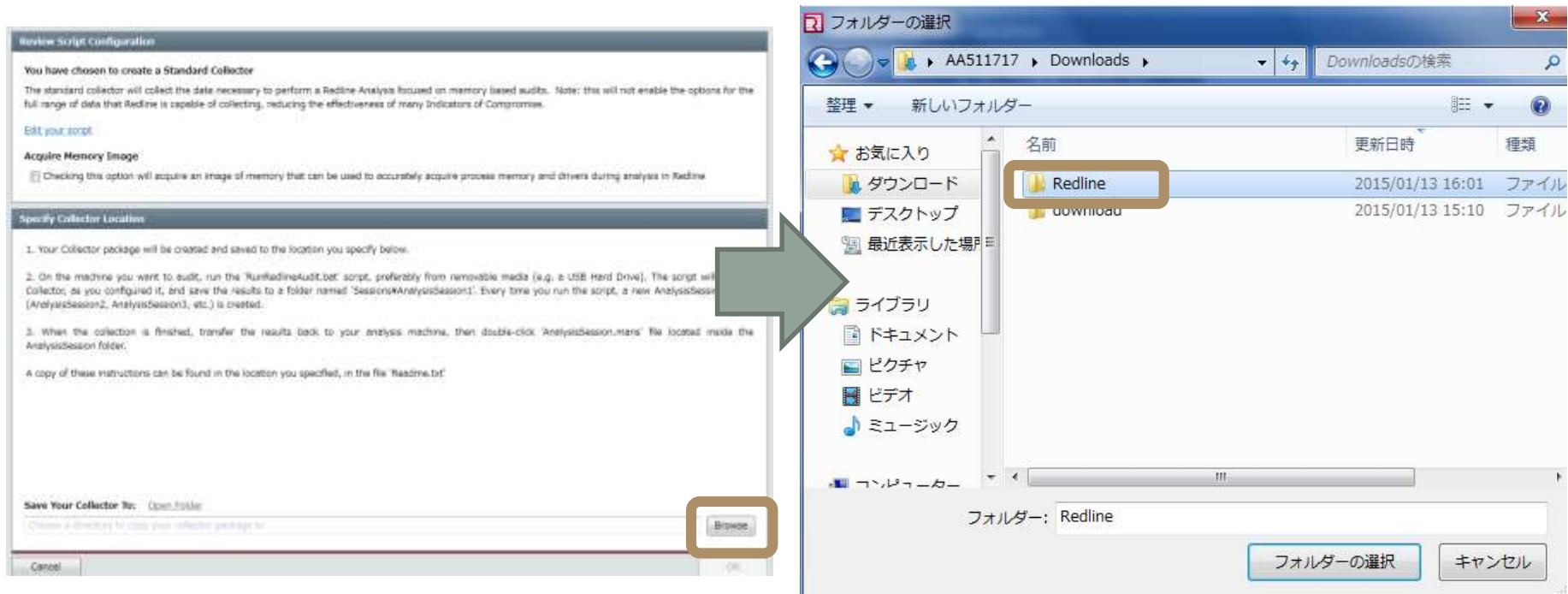
①Redline分析モジュールの作成手順

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



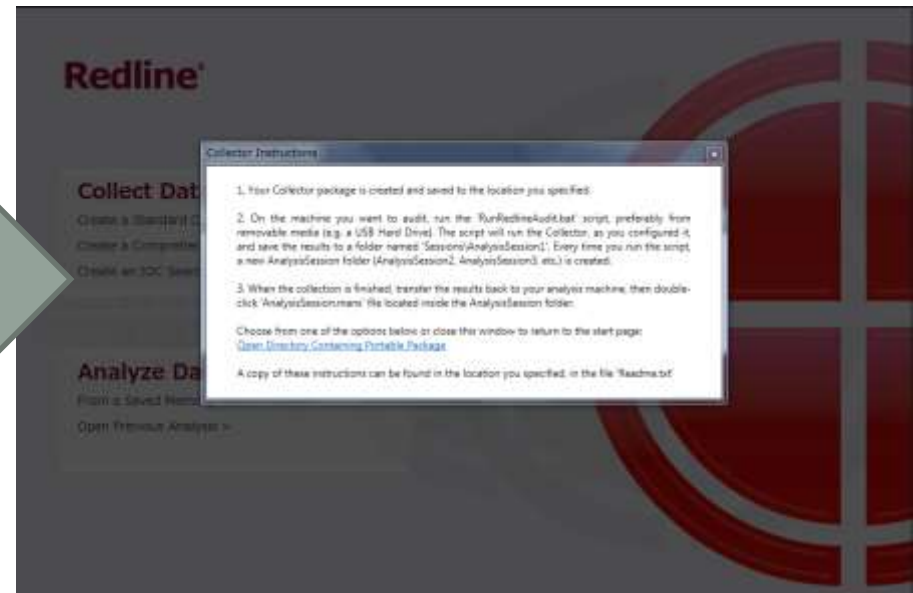
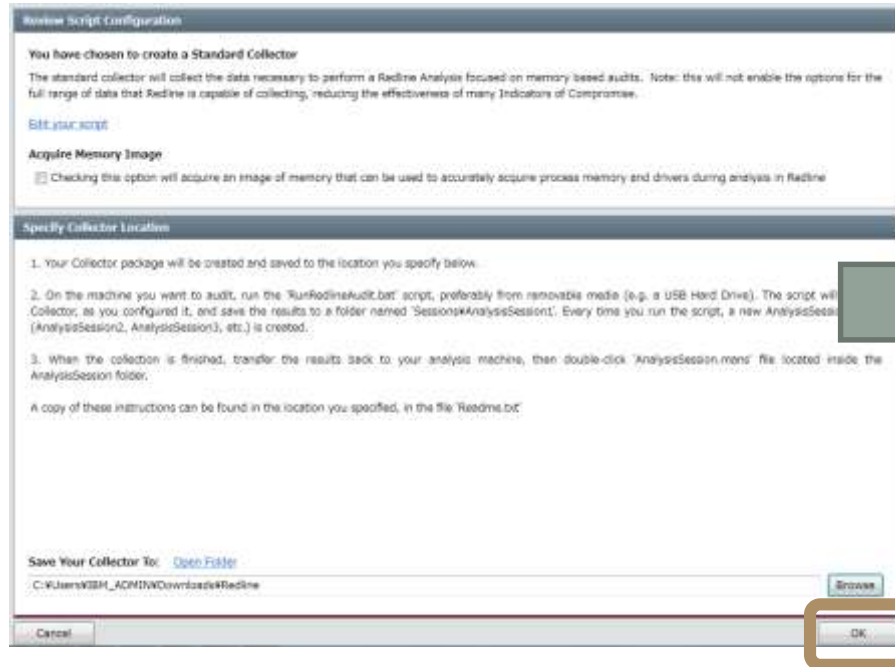
① Redline分析モジュールの作成手順

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。



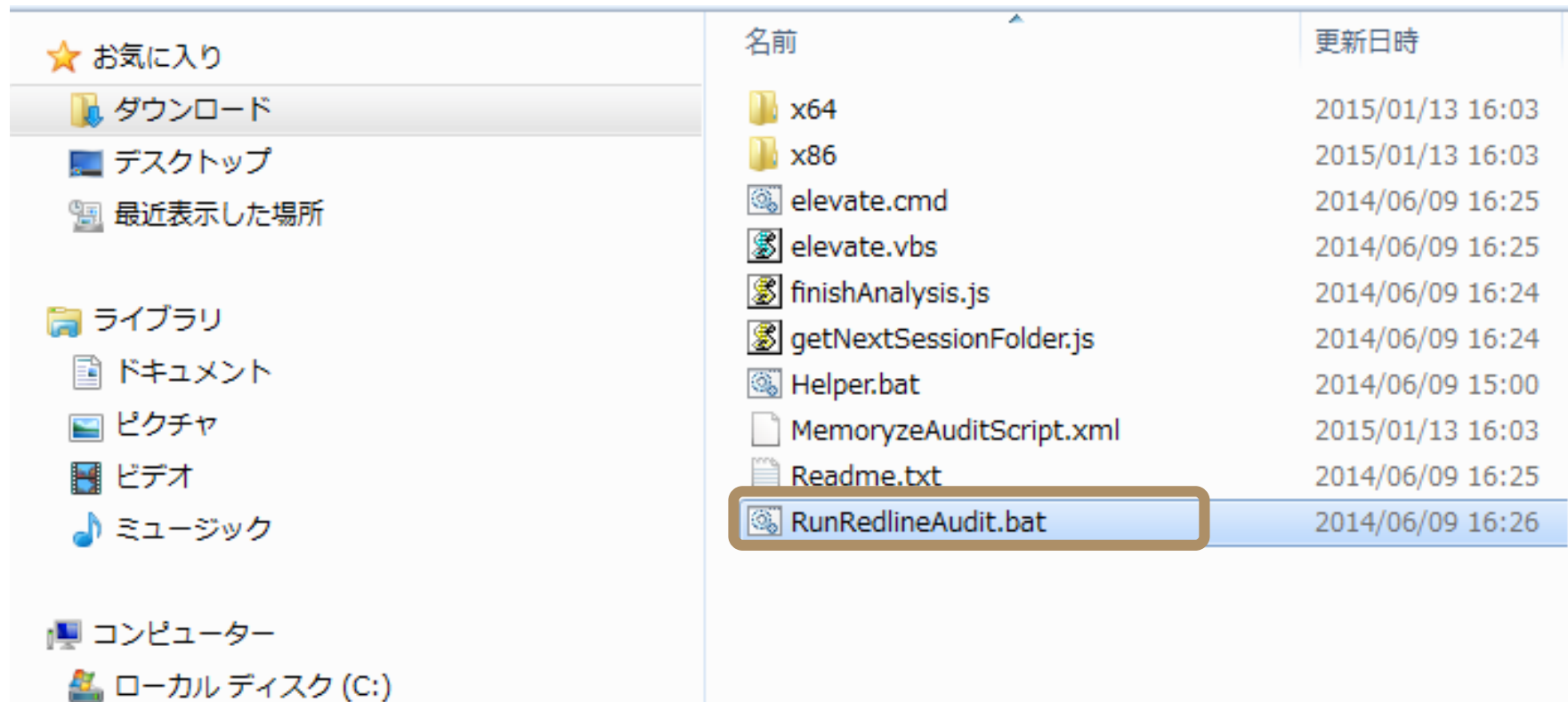
① Redline分析モジュールの作成手順

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。



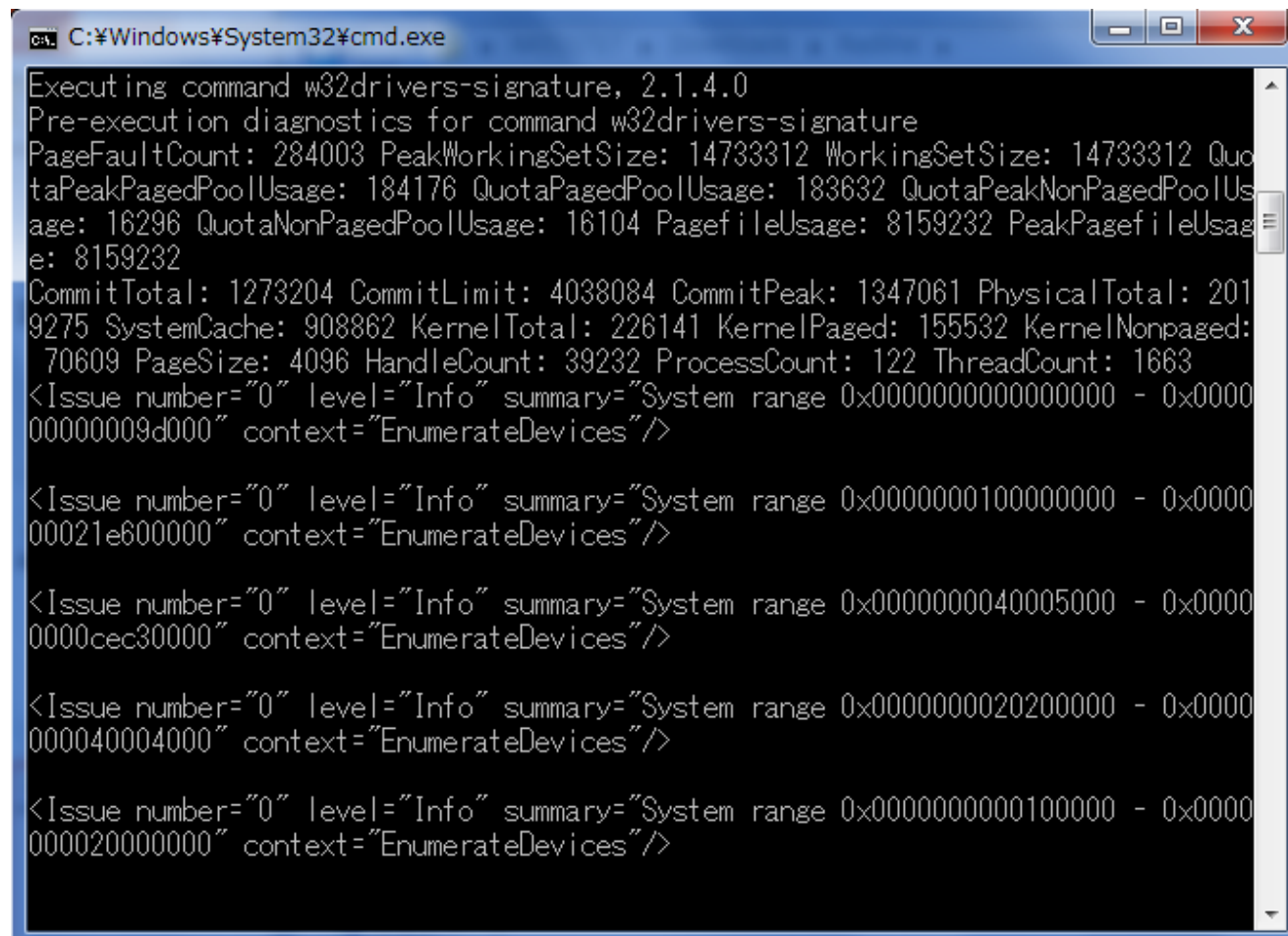
②Redline分析モジュールの使用手順

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。



②Redline分析モジュールの使用手順

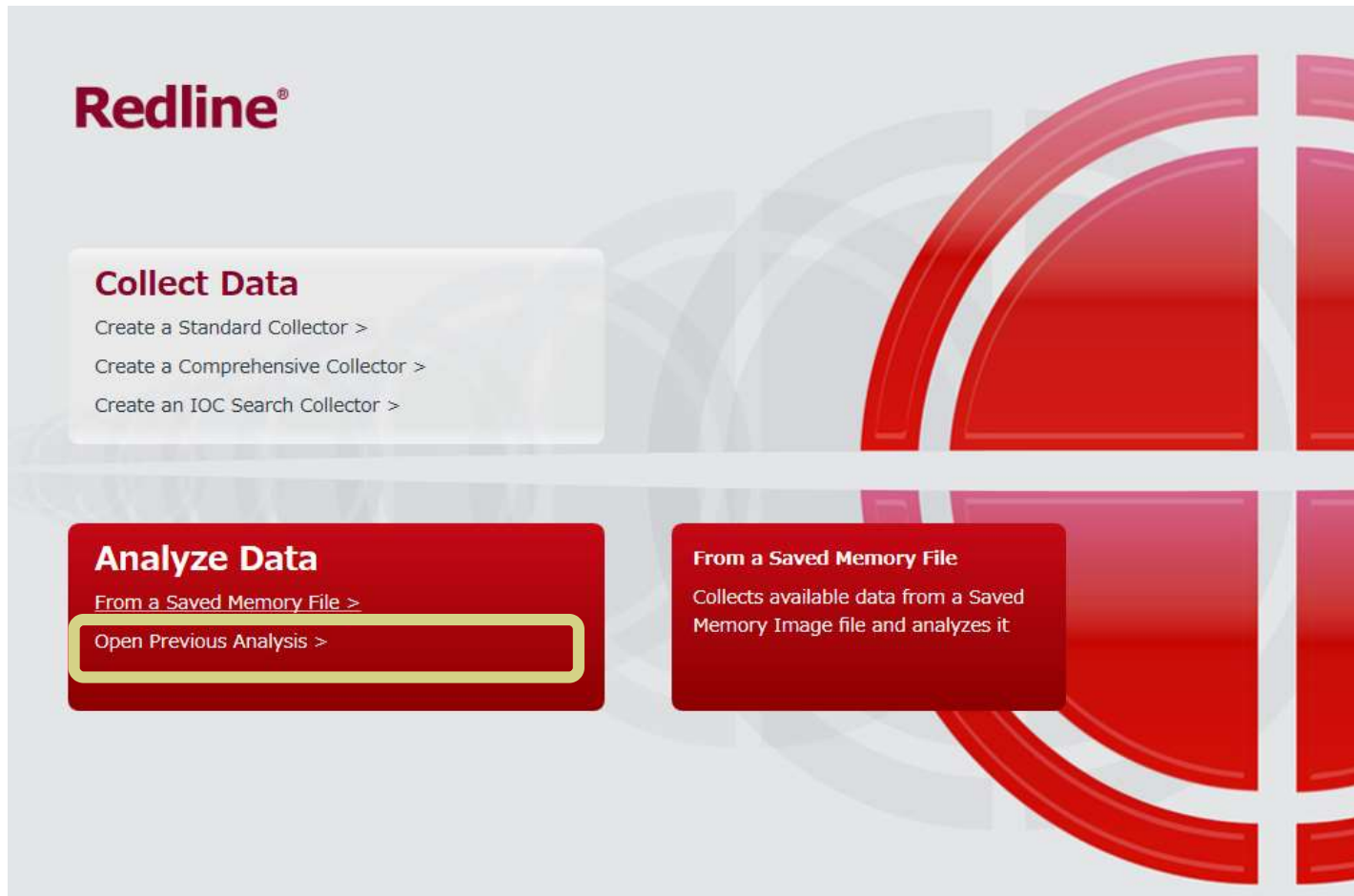
データの収集が開始されると図のような画面が起動します。



```
C:\Windows\System32\cmd.exe
Executing command w32drivers-signature, 2.1.4.0
Pre-execution diagnostics for command w32drivers-signature
PageFaultCount: 284003 PeakWorkingSetSize: 14733312 WorkingSetSize: 14733312 QuotaPeakPagedPoolUsage: 184176 QuotaPagedPoolUsage: 183632 QuotaPeakNonPagedPoolUsage: 16296 QuotaNonPagedPoolUsage: 16104 PagefileUsage: 8159232 PeakPagefileUsage: 8159232
CommitTotal: 1273204 CommitLimit: 4038084 CommitPeak: 1347061 PhysicalTotal: 2019275 SystemCache: 908862 KernelTotal: 226141 KernelPaged: 155532 KernelNonpaged: 70609 PageSize: 4096 HandleCount: 39232 ProcessCount: 122 ThreadCount: 1663
<Issue number="0" level="Info" summary="System range 0x0000000000000000 - 0x0000000000000009d000" context="EnumerateDevices"/>
<Issue number="0" level="Info" summary="System range 0x000000001000000000 - 0x0000000000000021e60000" context="EnumerateDevices"/>
<Issue number="0" level="Info" summary="System range 0x000000000400050000 - 0x0000000000000000cec30000" context="EnumerateDevices"/>
<Issue number="0" level="Info" summary="System range 0x000000000202000000 - 0x000000000000000040004000" context="EnumerateDevices"/>
<Issue number="0" level="Info" summary="System range 0x000000000001000000 - 0x000000000000000020000000" context="EnumerateDevices"/>
```

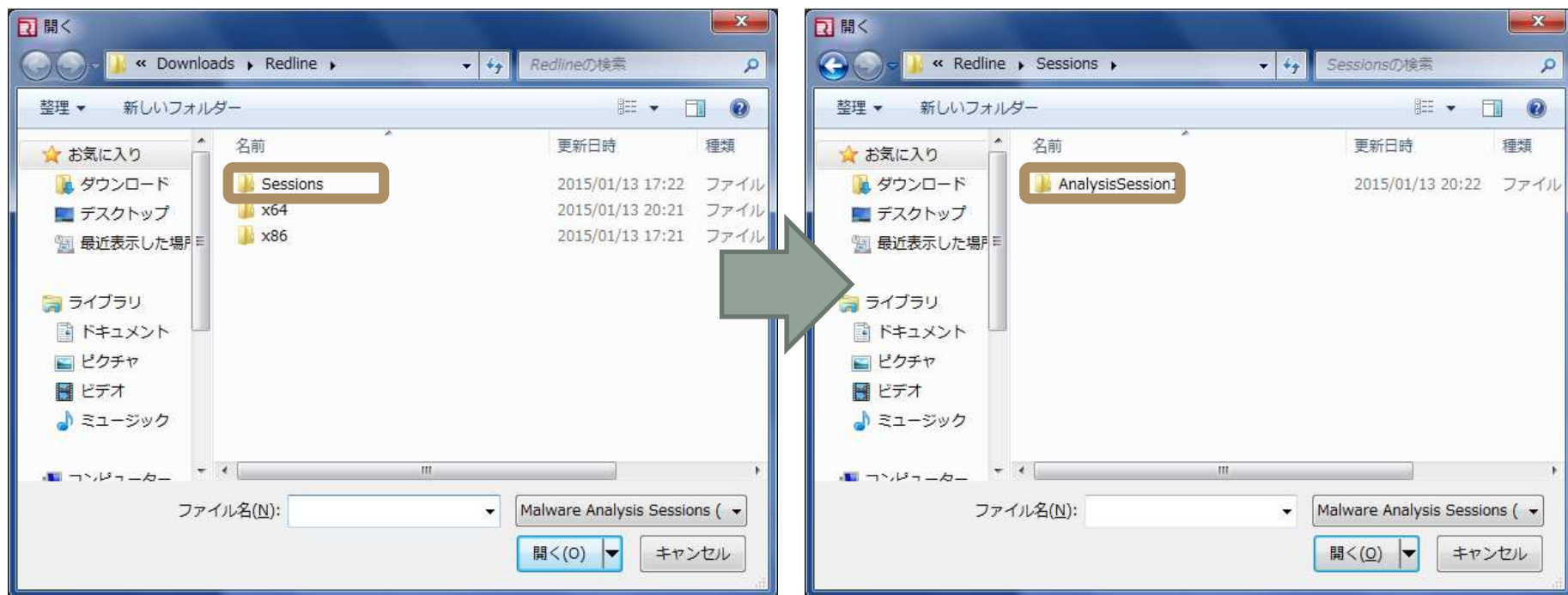
③Redlineによる調査手順

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。



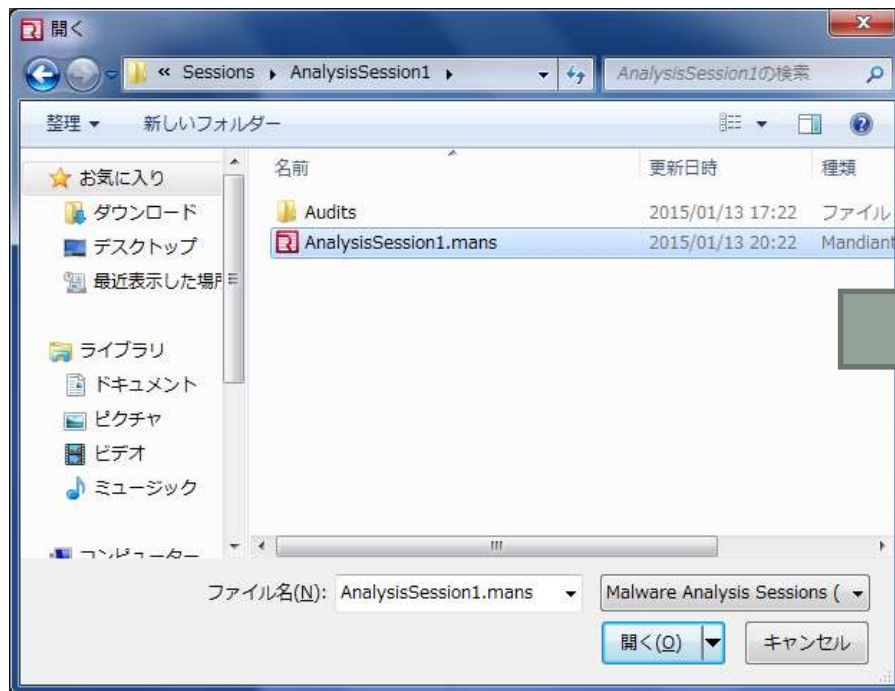
③Redlineによる調査手順

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。



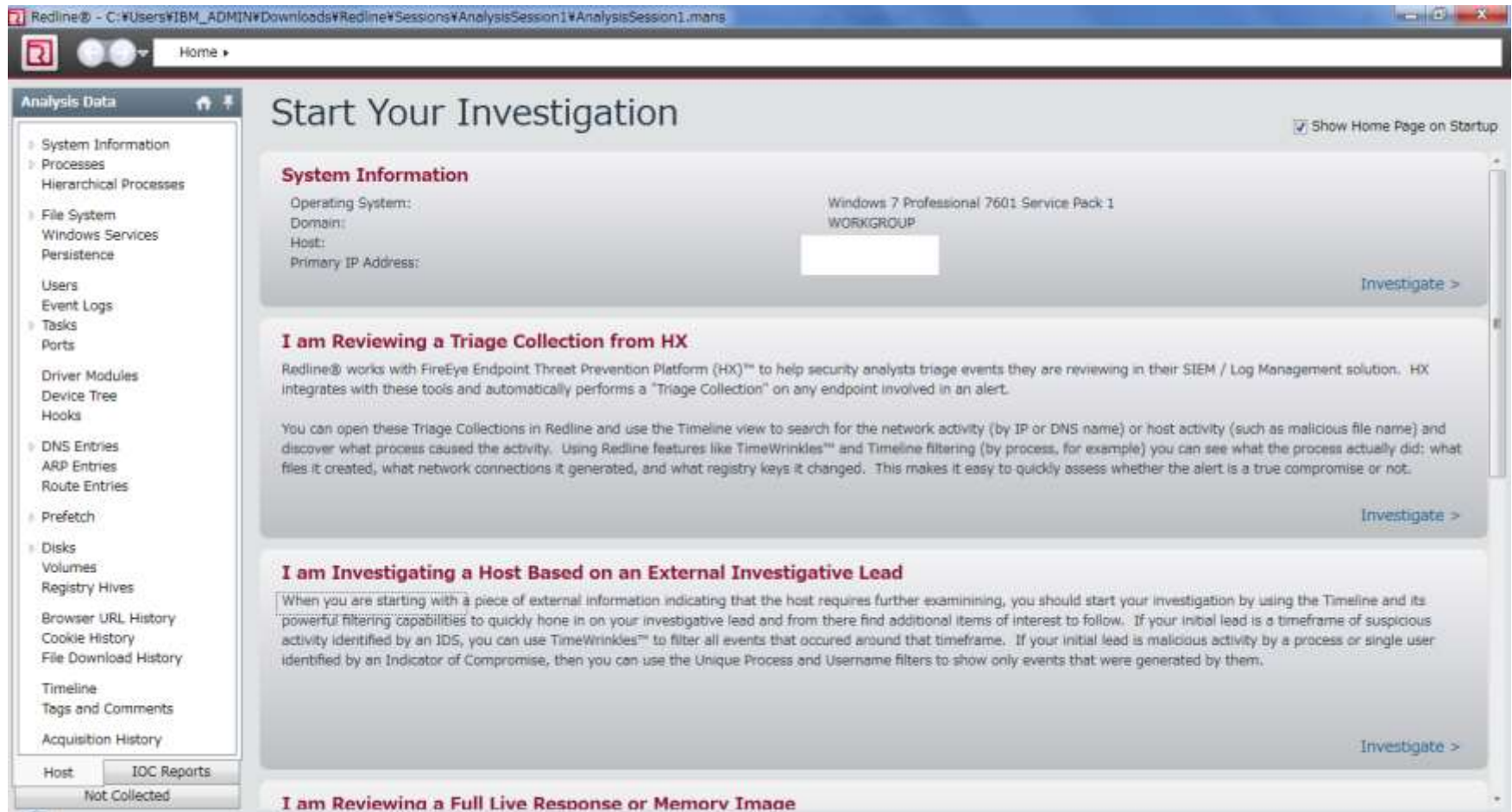
③Redlineによる調査手順

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。

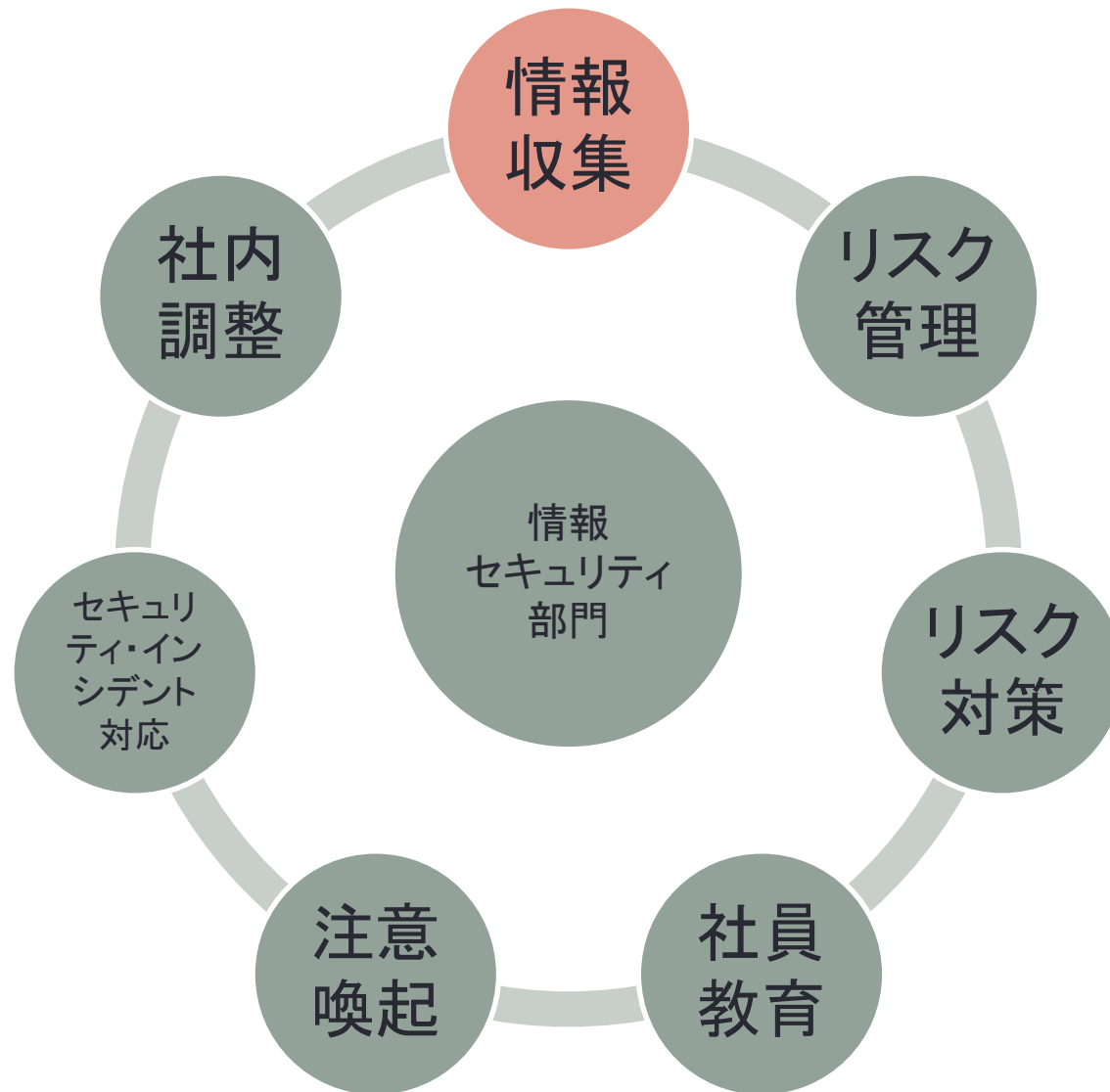


③Redlineによる調査手順

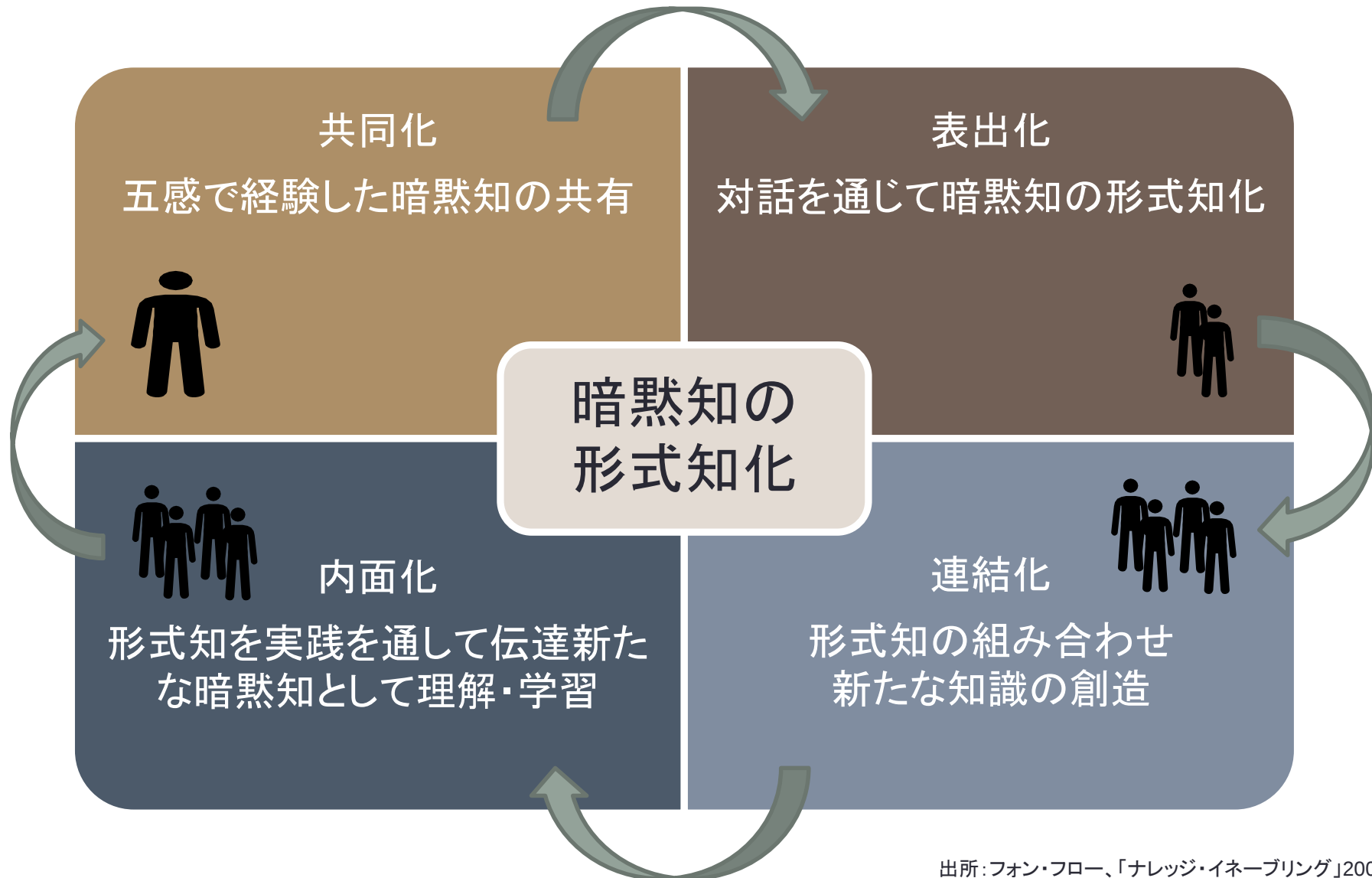
データの読み込みが完了すると、以下のような画面が表示されます。



情報セキュリティ部門の業務範囲



知識創造



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:

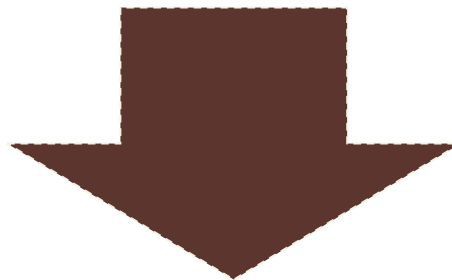
複数の企業でインシデント事例を分析する事により『効率的な対応』や『効果的な対策』が導き出せることを目的とし、社内および社外への連絡方法、社内体制(法務、営業など)、効果的な再発防止策に関する分析を行う。

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

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。