情報セキュリティ内部監査読本
初学者向け
（入門編）

2024年8月11日

本書の位置付け

昨今のサイバー攻撃における被害状況の実態は報道される以上に深刻さを増してきており、主に海外からの無差別な攻撃によって大企業のみならず中小企業、小規模事業者においてもランサムウエアなどによる情報漏えい、業務停止など企業存続に極めて重大な危機をもたらしています。
国や産業界においても、サプライチェーンに連なる中小企業が被害を受けることによって大手企業の製造ラインがストップしてしまうことや、取引先の中小企業を踏み台にした大手企業への標的型攻撃が行われていること等を踏まえ、企業規模に関わりなく、一定レベルの情報セキュリティ対策（外部攻撃や内部不正対策）とその実施状況の点検（監査）の必要性を求める動きとなってきています。

このような背景を受け、JASAとJNSAは、社内に監査の専門家がいないケースや、新たに情報セキュリティの監査を担当することになった方、（また取引先（発注先）中小企業の情報セキュリティ監査（外部監査）を担当することになった方）などを対象として、本書を作成いたしました。
これまでに情報セキュリティ監査を受けたことも実施したこともない方やこれから情報セキュリティ監査を実施しなければならない立場になった方向けに情報セキュリティ監査とは何か？どういうことをやるのかについてわかりやすく全体像を示す羅針盤的な位置付けの資料となっています。

本書が次のステップへの第一歩になれば幸いです。

情報セキュリティ監査の必要性

本書の位置付けに記載したようにサイバー攻撃やサプライチェーンの問題から企業を守る観点で、経営者が担う役割は非常に重要となります。情報セキュリティ対策においても、企業として対処すべきリスクを明確にし、組織に属する者が同じ目線で対策ができるように、経営者として「リーダーシップの発揮」が求められます。

リーダーシップを発揮するためには、組織における情報セキュリティ対策の実態を正しく把握することが必要です。経営者の考え方が末端まで浸透しているのか、ルールは適切に設定され、皆がそれに従っているのかなどを常にモニターしておくことで、新たな脅威やぜい弱性に対応することができます。また、適切な技術を導入すると共に、それが正しく運用されていること※の確認も必要です。

モニタリングの結果に基づいて、現場に寄り添ったルール設定を行うと共に、役職員の意識の向上を図り、技術的面では運用を徹底することで、より確実なセキュリティ対策が行えます。

モニタリングのために各事業部や部門に対してアンケート等を実施してセルフチェックするのも一つの方法ですが、責務を負う人達の自己採点のため、人により甘め・辛めのブレがあり、同じ状況か否かが分かりません。客観的な事実把握のために、監査人を育成して組織の状況を同じ基準で評価することをお勧めします。

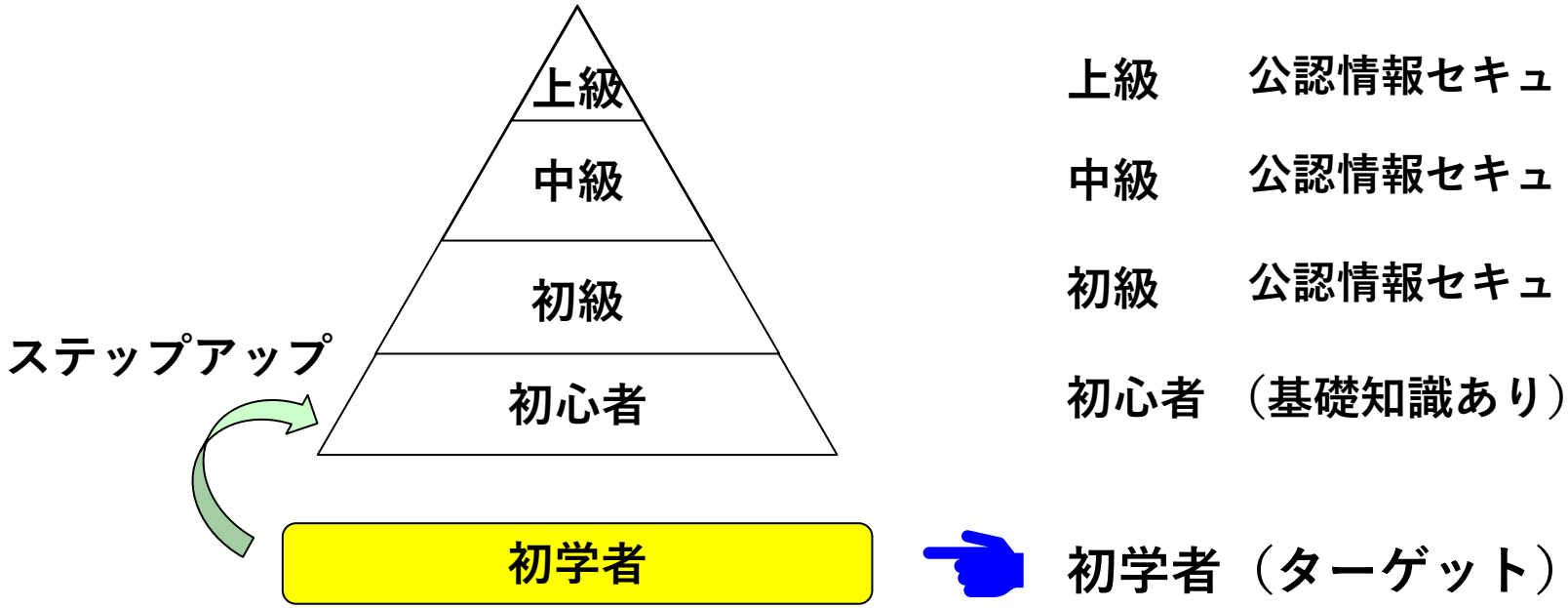
第三者として対象組織の状況を評価する内部監査人を通じて、組織の各部の状況を的確に把握して、致命傷となりえる箇所を発見し、より優先度の高いところから対策を実施していきませんか？

※ 例えば、最新のサイバー攻撃の検知ツールを導入しても、適切に運用されていないと機能しません。ツールを全端末に導入することはもちろん、端末の入れ替えが発生した場合には抜け漏れが無いように運用する必要があります。また、検知した異常に対してタイムリーに対処する運用を適切に実施する必要もあります。

本書を作成した目的

これまでに情報セキュリティ内部監査（以下、本書では「内部監査」と略す）を受けたことも実施したこともない方に向けて内部監査についての概要を理解しやすいように構成しました。正確性や厳密性ではなく内部監査というものがどういうものか朧げにでも理解して情報セキュリティの内部監査の読本や研修を受講する前の頭の整理の位置付けになります。

次のステップへの第一歩になれば幸いです。



上級　公認情報セキュリティ主任監査人

中級　公認情報セキュリティ監査人

初級　公認情報セキュリティ監査人補

初心者（基礎知識あり）

初学者（ターゲット）

JASA 情報セキュリティ監査制度体系

本書の構成と初学者にお伝えしたいポイント

入門者（初学者）に知って欲しいこと　３つ

１．監査とは？

・「監査」の概念
・第三者チェックの必要性
・監査の成り立ち
・情報セキュリティ監査とは（会計監査との簡単比較）
・監査の種類（外部監査、内部監査、自己点検）

２．内部監査の全体像

・監査の全体像とステークホルダー（関係者の繋がり）
・監査手続きの流れ
・監査人の心得

３．内部監査の事例

・代表的なユースケース
・監査チェックリストの事例紹介

1．監査とは？

「監査」の概念

組織目標を達成する上で阻害要因となるセキュリティリスクへの対策が有効に働いているかどうか判断するために、その対策の立案や実施に係らない第三者（監査人）が、セキュリティ対策として定めたルール及びルールに基づく行為を、一定の基準に基づいて客観的に評価すること

（注1）情報セキュリティ：情報の機密性・完全性・可用性を守ること

（注2）一定の基準：評価対象となる事項に係る人（被監査主体）や評価結果を用いて対策等の見直しなどを行う人（監査利用者）が合理的であると認める客観的な指標。ベストプラクティス（ISO規格）などに基づき作成される。社内規定が妥当であると認められる場合には、社内規定を基準とすることもできる。

1．監査とは？（監査の歴史は古くから）

古代ギリシャの都市国家には、公会計の計算書の監査に関し整備された仕組みとして10名程度で構成する監査局というものがあり、
最高権力機関として執政官が退任する際に、会計書類の提出を求め、それまで行った会計処理が適切であることを確認していたという研究報告（※）がある

・現代の要請だけでなく古代ギリシャの都市国家でも同様の監査の仕組みがあった

・独立した組織による第三者評価

・感覚やフィーリングによる確認ではなく、データ（会計書類）による客観的な評価

・監査の受け手（被監査主体）と監査人、結果の利用者（報告書利用者）に共通する基準に基づく評価

誰もが納得できる第三者による公正な評価が有意義です

※ 会計史の文献が古代にも紙幅を割いている 意味についての一考察（百合野 正博）

https://doshisha.repo.nii.ac.jp/?action=repository_action_common_download&item_id=15144&item_no=1&attribute_id=28&file_no=1

1．監査とは？（第三者の評価の必要性）

何故、第三者による評価が大事なのか？

◯何故、対策の評価が大事なのか？

・大切に管理しないといけない個人情報や会社の機密情報がどのように守られているか（どのように管理しているか）について、対策の実施状況を評価することで、対策の不具合もいい面も把握することができます。
・不具合があれば対策を見直し、いい面は組織全体で共有することで、より効果があり、より負担の軽い対策ができるようになります。

◯何故、第三者による評価が求められるのか？

・自己評価では、思い込みや理解不足は発見できません。更に、ミスを隠そうとする人もいるので、実情が分かりにくいです。
・第三者が客観的に評価すると、良しにつけ悪しきにつけ、実態が的確に分かります。
・的確な実態把握により、効果的に改善できます 。

だから、誰もが納得できる第三者による公正な評価が有意義です

1．情報セキュリティ監査とは（会計監査との簡単比較）

分類	会計監査	情報セキュリティ監査
目的	決算書をはじめとした財務諸表を対象に、会計処理とその記載の適正性を証明し、報告すること	情報セキュリティに係るリスクマネジメントが効果的に実施されるように、ルールの整備や運用状 況を検証又は評価して、報告すること（保証型監査あるいは助言型監査）※
確認事項	作成した財務諸表や計算書類について、法令や規則に則った記載内容になっているかどうかを検証すること	適正なルールが整備されているか？ 設定したルール（基準）に従った運用が適切に実施されているか（適合性の確認）
評価結果	無限定適正意見：適正 限定付適正意見：一部改善すべき問題があるものの、概ね適正 不適正意見：財務諸表が適正でない 意見不表明：何らかの理由により、適正か否かの判断ができない	適合/不適合 改善事項
実施者	監査法人や公認会計士	情報セキュリティ監査人

目的や実施者はことなりますが、どちらも「ルールが整備され、ルールに従っているか」を確認する行為です

※ 詳細は次頁参照

※ 保証型監査と助言型監査について

	保証型監査	助言型監査
概要	監査の対象となる組織体の情報セキュリティに関するマネジメントやマネジメントにおけるコントロールが監査手続きを実施した限りにおいて適切である旨を伝達する監査の形態	監査対象となる組織体の情報セキュリティに関するマネジメントや、コントロールの改善を目的として、監査対象の情報セキュリティ上の問題点を検出し、必要に応じて当該検出事項に対応した改善提言を行う監査の形態
備考	「保証」といっても、結果としてインシデントが発生しないという絶対的な保証ではなく、一定の判断の尺度に従って監査手続きを行った範囲における合理的な保証となることに留意	

＊＊＊　JASAのサイトより引用　＊＊＊

https://www.jasa.jp/audit/about/about02/

1．監査の種類（外部監査、内部監査、自己点検）

分類	外部監査	内部監査	自己点検
目的	組織が外部の利害関係者に、情報セキュリティ対策の有効性を説明するために行う	組織が、自ら行っている情報セキュリティ対策の有効性を評価し、よりよい対策とするために行う	情報セキュリティルールの順守について日々の業務プロセスの中で確認し、自ら是正する
確認項目	情報セキュリティに係る規程類などのルールに基づき遵守状況を確認 情報セキュリティマネジメントが有効に働いているか確認	同左	点検のチェックリストに基づき確認を行う
確認方法	文書審査 インタビュー エビデンス（証跡）	同左	点件のチェックリストに基づくセルフチェック
確認する人	外部の情報セキュリティサービス事業者 認証機関の審査員など	自組織内の利害関係の無い組織に所属する内部監査員 業務プロセスを実施する作業者	業務プロセス担当者・責任者
監査結果を利用する人	顧客、株主、その他外部の利害関係者	組織経営者	業務プロセスの担当者／責任者

本書の説明する範囲

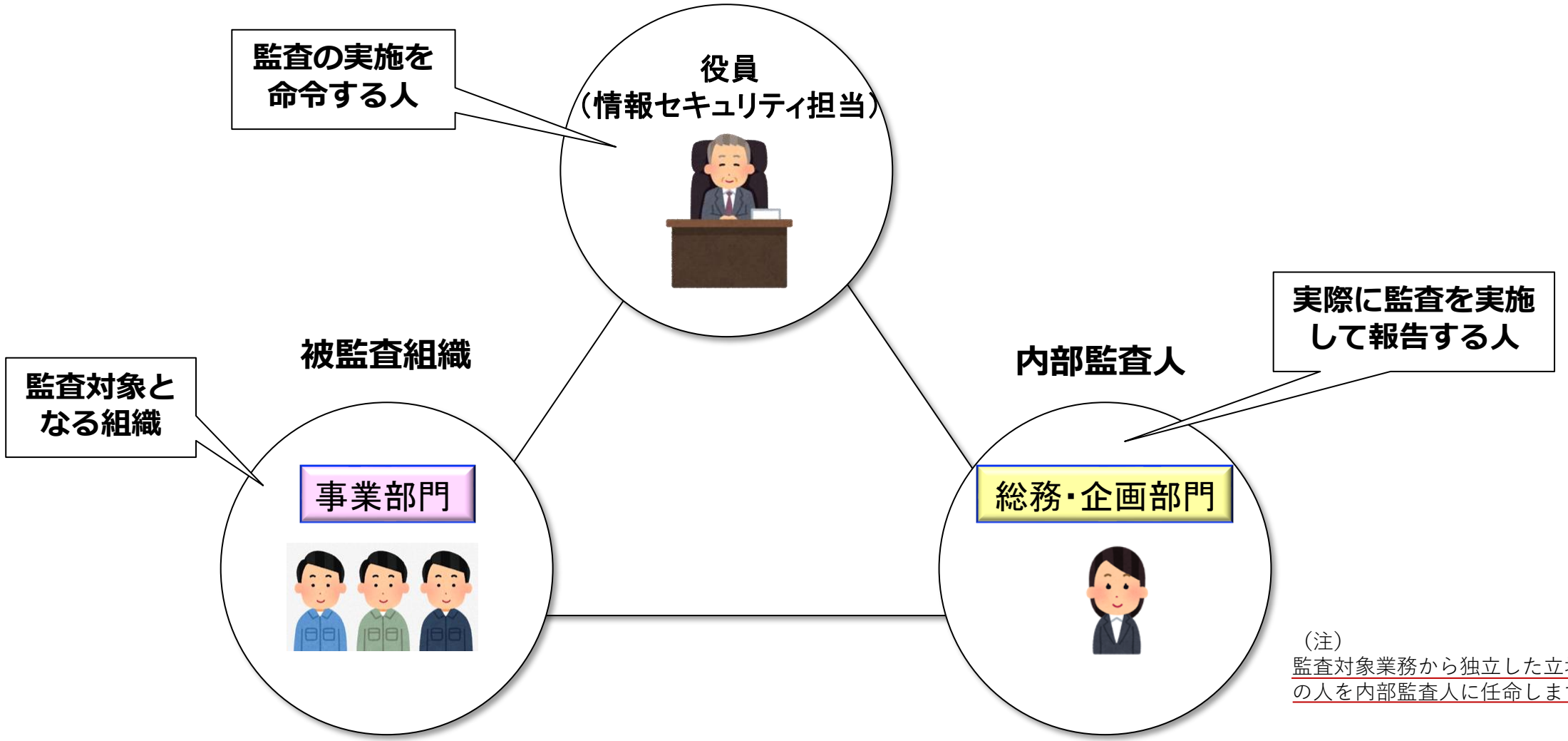
2．内部監査の全体像

2．監査の全体像（監査手続の流れ）

NO	監査手続の項目	概要＆補足説明
①	内部監査の指示＆監査人の任命	内部監査の指示は組織の長（社長など）により正式に通達されて行われます（監査人の任命も）
②	内部監査計画書作成	何の目的でどのようなことをどのくらいの期間で実施するか計画書を作成します
③	対象組織への通知＆日程調整	関係者に一定の時間（2～3時間）の予定を空けてもらってヒアリングするので業務への影響が少ない日程を調整
④	内部監査の実施 ・記録の確認 ・インタビュー ・結果の記録など	組織で策定したルールに従っているか記録を確認したり、インタビューで確認をします ※ 事例は項番３．内部監査の事例にて紹介
⑤	報告書作成	内部監査報告書として調査結果をまとめます
⑥	内部監査結果報告	報告書は内部監査の指示をした組織の長に報告をします
⑦	改善の指示	組織の長から発見されたルール逸脱箇所について改善の指示をします
⑧	改善計画の作成	内部監査で指摘された事項について改善計画を策定します

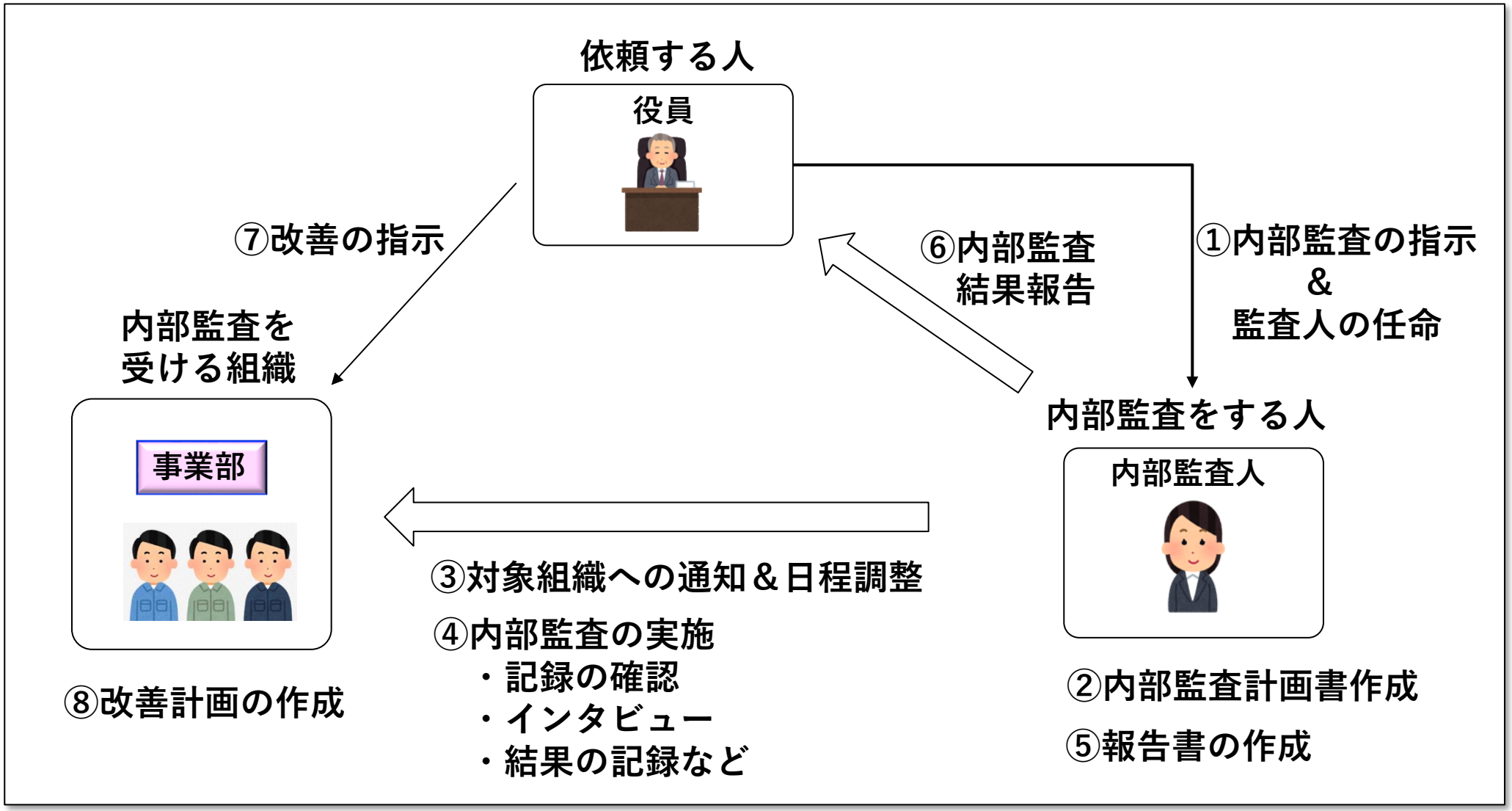
2．監査の全体像（ステークホルダー：登場人物）

主なステークホルダーは下記のようになります



（注）
監査対象業務から独立した立場の人を内部監査人に任命します

2．監査の全体像（監査手続の流れ）



（注）⑦、⑧は内部監査の結果の活用（内部監査の範囲外）

監査人の行動原則

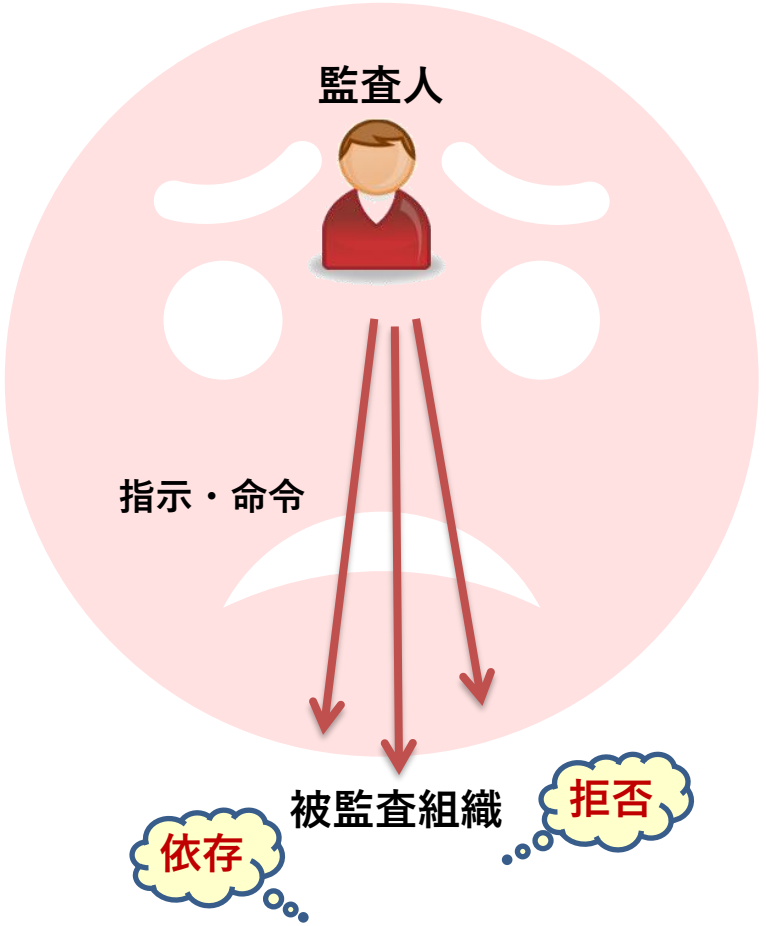
情報セキュリティの知識や監査スキルと同じくヒューマンスキルも大事！

（1）　自組織を見ない　-独立性-
（2）　公明正大であること
（3）　傾聴すること
（4）　客観性を大切に　-確実な証拠に基づいて-
（5）　サンプリングでバランスよく
（6）　タイムマネジメントを忘れずに！
（7）　助言を心がける　-改善への提案と優れた取り組みの推奨-

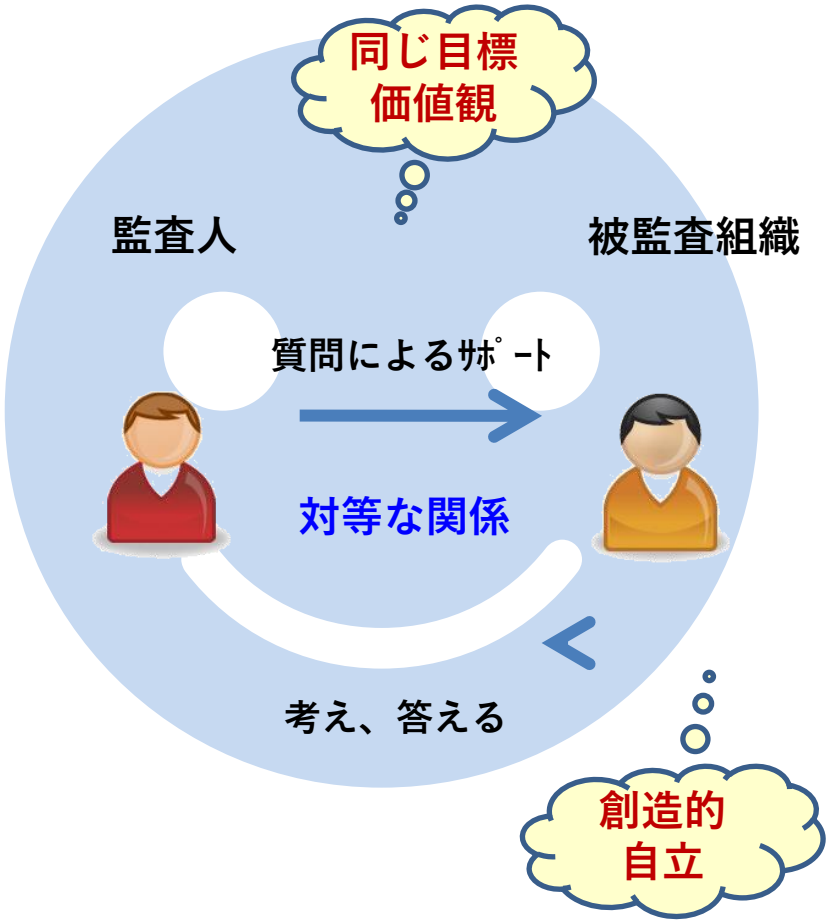
監査人の心得

被監査組織と監査人との関係は対等な立場であることを認識する

指示、命令系統ではなく、



質問による気づき



３．内部監査の事例

３．内部監査の事例（代表的なユースケース）

具体的な内部監査の事例として
ユースケースを使って説明を行います

（実際の事例を分かりやすくするために
身近な事例を出来るだけ簡略化して
要点を絞って説明を実施します）

今回の事例は主に④内部監査の実施についてご紹介します

依頼する人

役員

①内部監査の指示
&
監査人の任命

⑥内部監査
結果報告

⑦改善の指示

内部監査を
受ける組織

事業部

内部監査をする人

内部監査人

③対象組織への通知＆日程調整

②内部監査計画書作成

⑤報告書の作成

⑧改善計画の作成

④内部監査の実施
- 記録の確認
- インタビュー
- 結果の記録など

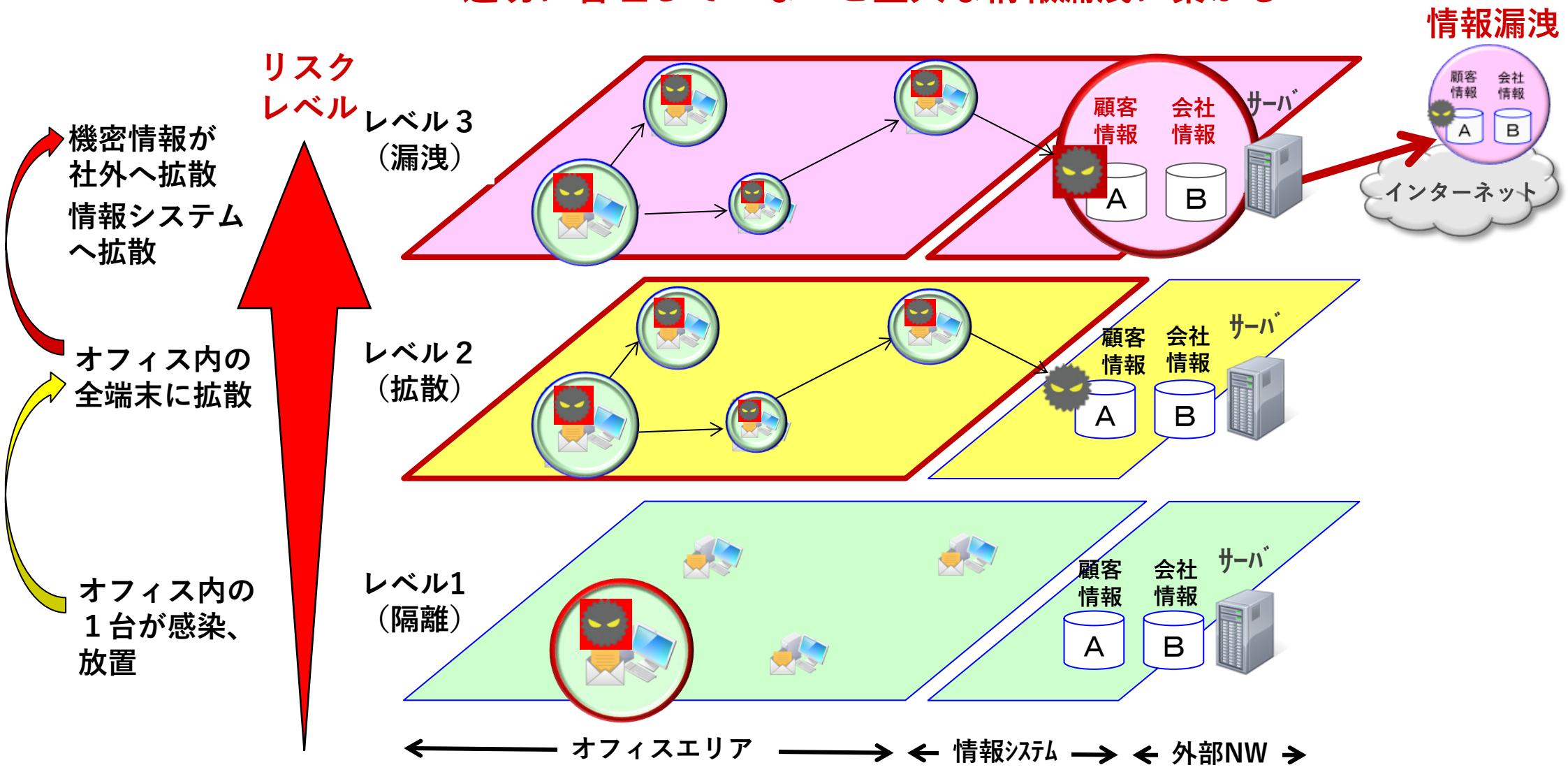
３．内部監査の事例（代表的なユースケース）

事例1：ウィルス対策ソフトの導入＆運用

今では入れることが常識となっているウィルス対策ソフトですが、導入されていなかったり適切に運用されていなかった場合に何が起こるのでしょうか？

ウィルス対策が適切に実施されていない場合の想定リスク

→ 適切に管理していないと重大な情報漏洩に繋がる



3．内部監査の事例（代表的なユースケース）

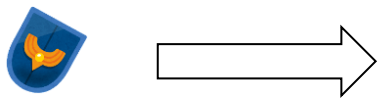
例）ウィルス対策ソフトの導入＆運用

◯会社のセキュリティ規則（抜粋）

マルウェア対策として以下項目を実施すること　・・・　基準（セキュリティルール）

① 利用しているPCすべてにウィルス対策ソフトを導入（インストール）すること
② ウィルス対策ソフトの定義ファイルを最新化すること
③ 毎週金曜日にフルスキャン（利用しているPCのHDDをすべて確認）すること

①ウィルス対策ソフト
のインストール

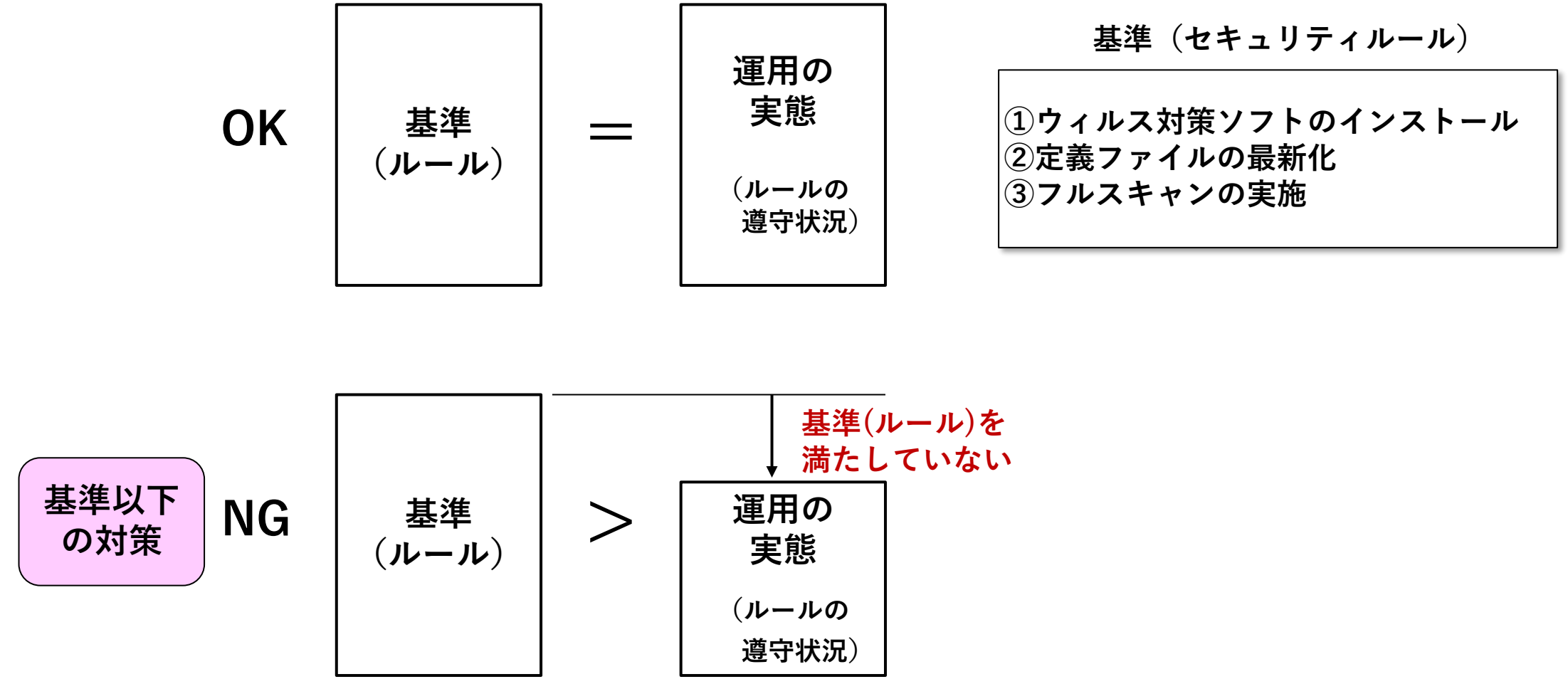


②定義ファイルの最新化

③フルスキャンの実施

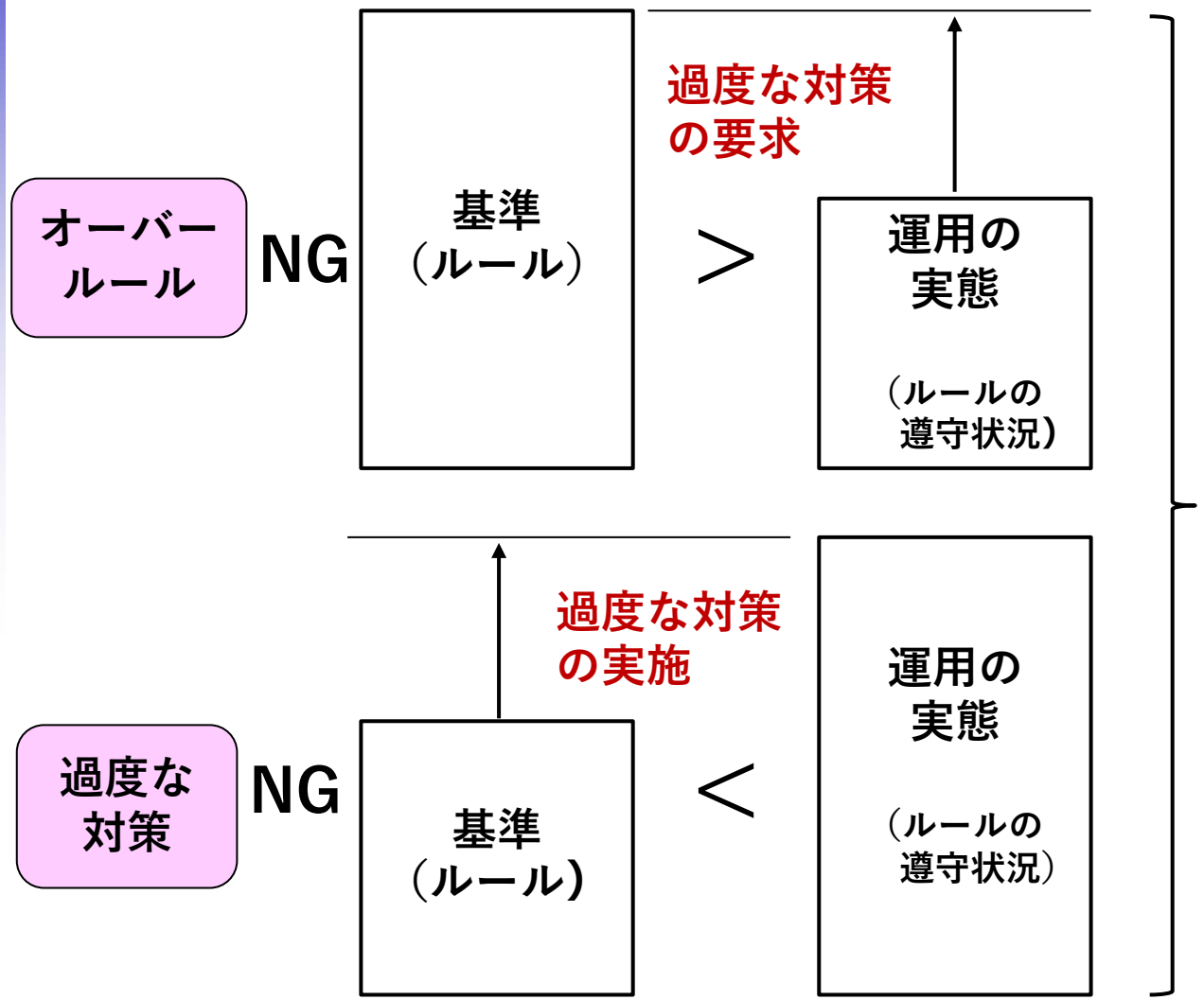
3．内部監査の事例（代表的なユースケース）

基準（セキュリティルール）に照らし合わせて対策状況を確認する



3．内部監査の事例（代表的なユースケース）

オーバールールや過度の対策の有無を確認する



基準（セキュリティルール）

①ウィルス対策ソフトのインストール
②定義ファイルの最新化
③フルスキャンの実施

③フルスキャンを利用前に毎回実施するなどのルール設定や対策の実施を行うことで業務に影響を与えるので過度な要求や対策の実施がないかの確認も必要となることがある

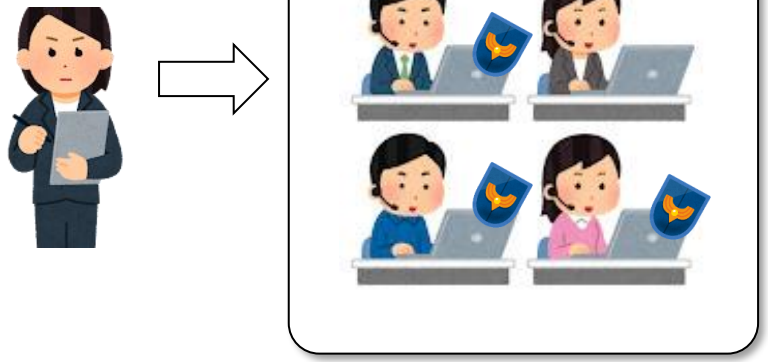
3．内部監査の事例（代表的なユースケース）

例）ウィルス対策ソフトの導入＆運用の観点での確認

被監査組織：Aの利用PC数は4台だったので
全数確認を実施しました
確認結果は下記の通りです

被監査組織：A

内部監査人



監査の基準と社内ルール

基準（確認項目）	詳細内容（社内ルール）
①ウィルス対策ソフトのインストール	ネットワークに接続するホストにはすべて指定のウィルス対策ソフトをインストールする
②定義ファイルの最新化	ウィルス対策ソフトのウィルス定義ファイルは常に最新のものを使用する
③フルスキャンの実施	クライアントについては原則、毎週末にフルスキャンを行う

チェックリスト＆確認結果

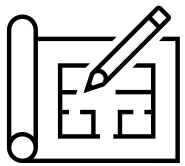
確認項目	PC #01	PC #02	PC #03	PC #04
①ウィルス対策ソフトのインストール	○	×	○	○
②定義ファイルの最新化	○	×	○	○
③フルスキャンの実施	×	×	○	×

事例：確認結果と簡易分析＆フォローアップ

チェックリスト＆確認結果

確認項目	PC #01	PC #02	PC #03	PC #04
①ウィルス対策ソフトのインストール	○	×	○	○
②定義ファイルの最新化	○	×	○	○
③フルスキャンの実施	×	×	○	×

発見事項について2点



発見1：PC #02はウィルス対策ソフト自体がインストールされていなかった

発見2：フルスキャンされていなかったPCが2台存在（PC #01、PC #04）

事例：確認結果と簡易分析＆フォローアップ

発見事項と要因分析＆是正対応

発見事項	指示事項	ルール逸脱の要因 （ヒアリング結果）	是正対応
発見1： PC #02はウィルス対策ソフト自体がインストール されていなかった	ウィルス対策ソフトのインストールの実施＆フルスキャンの実施	PCを新機種に交換したタイミングでウィルス対策ソフトのインストールをしない状態で利用していた	（例示） 機種交換時の設定マニュアルにウィルス対策ソフト等のインストールチェックリストを用意すると共にインストール結果＆設定状況のエビデンスの提出を行うプロセスとする
発見2： フルスキャンされていなかったPCが2台存在 （PC #01、PC #04）	フルスキャンの実施	フルスキャンのタイミングが金曜日に設定されており、実行すると終了するまで30分～1時間程度を要することとPCの反応が鈍くなることから業務優先で実行しなかった 特に金曜日は休み前のためにバタバタしていて他の曜日よりも余裕がない	（例示） フルスキャンのタイミングについて金曜日から水曜日に変更すると共に設定で昼休み等に実行するように設定を行う

事例：チェックリスト（サンプル）

実際に使用されているチェックリストのサンプル事例です。確認事項と確認方法、監査証拠をもとにインタビューを実施します。確認結果や確認内容も記載できるようにしています。

社内のセキュリティルール（監査の基準）		組織全体	個別	重点項目	確認事項	確認方法	監査証拠	確認結果	判定（※1）	確認内容（コメント）
No.	項　目									
2	マルウェア[注]の検出対策としてウイルス対策ソフトを導入し、適切に運用（定期的なフルスキャンなどのウィルスチェック）し、維持（最新の状態）すること 注：マルウェア＝コンピュータウイルス、ワーム、スパイウェア、トロイの木馬など不正な意図で作成された悪意のあるソフトウェアや悪質なコードの総称		○	○	**① マルウェアの検出対策としてウイルス対策ソフトをインストールしているか？**	監査対象PCにウィルス対策ソフトがインストールがされていて正常に動作していること	ウィルス対策ソフトの起動画面のキャプチャ	5台OK 1台NG	△	PCを新機種に交換したタイミングでウィルス対策ソフトのインストールをしない状態で利用していた
					②ウィルス定義ファイルを常に最新化しているか？ 監査時点での最新の定義ファイルになっているか？	監査対象のPCの定義ファイルが直近の最新の定義ファイルと比較して同一か直近のものとなっていること	監査対象PCの定義ファイルの番号や更新日と最新の定義ファイルの情報	4台OK 1台対象外	○	
					③定期的にフルスキャンを実施しているか？ 毎週金曜にフルスキャンを実施しているか？	ウィルス対策ソフトのログを確認し、フスキャンが実施されているか確認する（実施の有無、実施日）	監査対象PCのログ情報	1台OK 3台NG 1台対象外	×	フルスキャンのタイミングが金曜日に設定されており、実行すると終了するまで30分～1時間程度を要することとPCの反応が鈍くなることから業務優先で実行しなかった 特に金曜日は休み前のためにバタバタしていて他の曜日よりも余裕がない

※1　○：適合、×：重大な不適合、▲：軽微な不適合、△：改善の機会、－：対象外

執筆協力

・魚脇、尾崎、冨田、他JNSA/ISMS-UG有志メンバー
・JASA有志メンバー