大企業すら突破される時代のセキュリティ評価制度対策
～中小企業の生き残り戦略～

取引停止リスクを回避したい中小企業のための
セキュリティ対策 実践ガイド

セキュリティ対策事例集付き

目次

サイバー攻撃の実態とセキュリティ評価制度

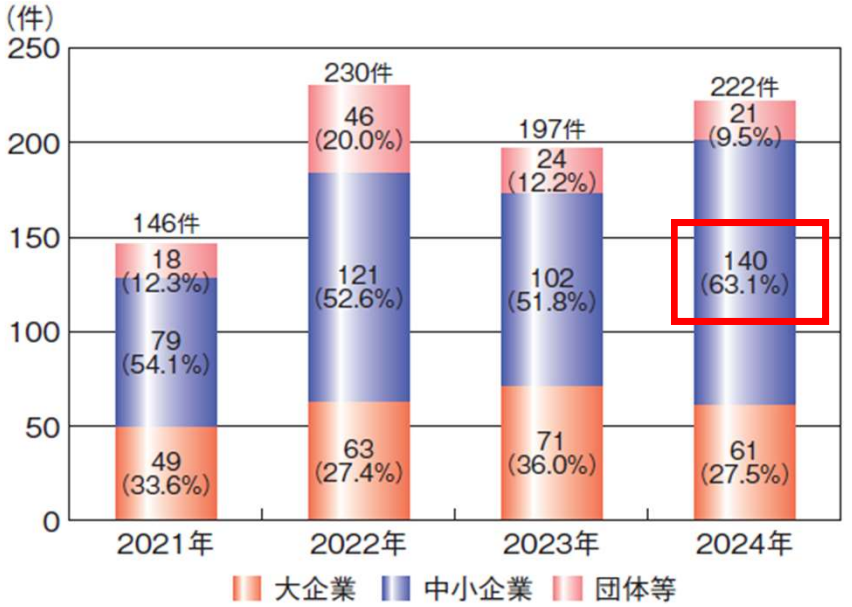
近年、サイバー攻撃の矛先はサプライチェーンの弱点である「中小企業」へと向かっています。2026年より始まる国の新制度により、大企業との取引を維持するための条件は変わろうとしています。

現代のサイバー攻撃は急激な進化を続けています。
様々なセキュリティ対策が生み出されているにもかかわらず、
被害が収まる兆しが見えません。
IPAの情報セキュリティ白書2025によると、国内のランサムウェアによる被害のうち、中小企業が約63%にも上ります。

大企業は高度なセキュリティ対策を施しているため、侵入は容易ではありません。
そのため、セキュリティの甘い中小企業の子会社や協力会社に侵入し、踏み台として大企業に侵入するサプライチェーン攻撃が主流になりつつあります。

セキュリティ対策が急務であり、経済産業省から2026年後半にも「セキュリティ対策評価制度」が施行予定です。
セキュリティ対策評価制度により、各企業のセキュリティ対策が★1～5で格付けされます。

国内のランサムウェアによる被害件数（2021～2024年）



出典：IPA 情報セキュリティ白書 2025 P14

入札条件や提案条件に格付けが活用されることが想定されており、中小企業であってもセキュリティ対策は必須といえます。

対策を阻む3つの壁

大企業が中小企業に求めるセキュリティ対策のレベルは高まっていますが、実現にはいくつもの課題があります。取引停止となるリスクを減らすためにもこの課題を解決しなければなりませんが、セキュリティ専門の部署を設置している中小企業は非常にまれです。

セキュリティ対策が後手に回る３つの理由

予算	要員	スキル
セキュリティ対策がコストと考えられ、十分な予算確保できない	人手不足が深刻化しており対策に当たる要員が足りない	サイバー攻撃に対して対策に必要なスキルが追い付かない

サプライチェーンセキュリティの対策は急務ですが、一朝一夕に解決できる問題ではない

経済産業省の情報セキュリティ評価制度においては取引先の管理が重要視されており、大企業が取引先に求める格付け「★3」になると想定されています。

Point

現地監査もあるため、実態として正しいセキュリティ対策の理解と運用が必要です。

効果の上がらないセキュリティ対策

予算・要員・スキルが不足する中でも対策を講じている企業はありますが、効果が上がらないケースは少なくありません。
主な原因は正確な現状把握ができていない点になります。

現状が把握できていない

どのような情報資産があり、どのようなリスクがあるか、正確にわからない

対策があっていない

情報資産が正確に把握できていないため、真に必要な対策が取れていない

対策費用が不足する

誤った施策により無駄なコストが発生し、本来の対策費用を圧迫する

失敗例：複数のセキュリティ機能を統合したUTM製品を勧められて導入

営業資料は社外で参照するため
クラウドに保存

UTMはインターネットとイントラネットの**境界を守る**製品

クラウドへの不正アクセスは、
UTMを経由しないため
効果的な投資になっていない

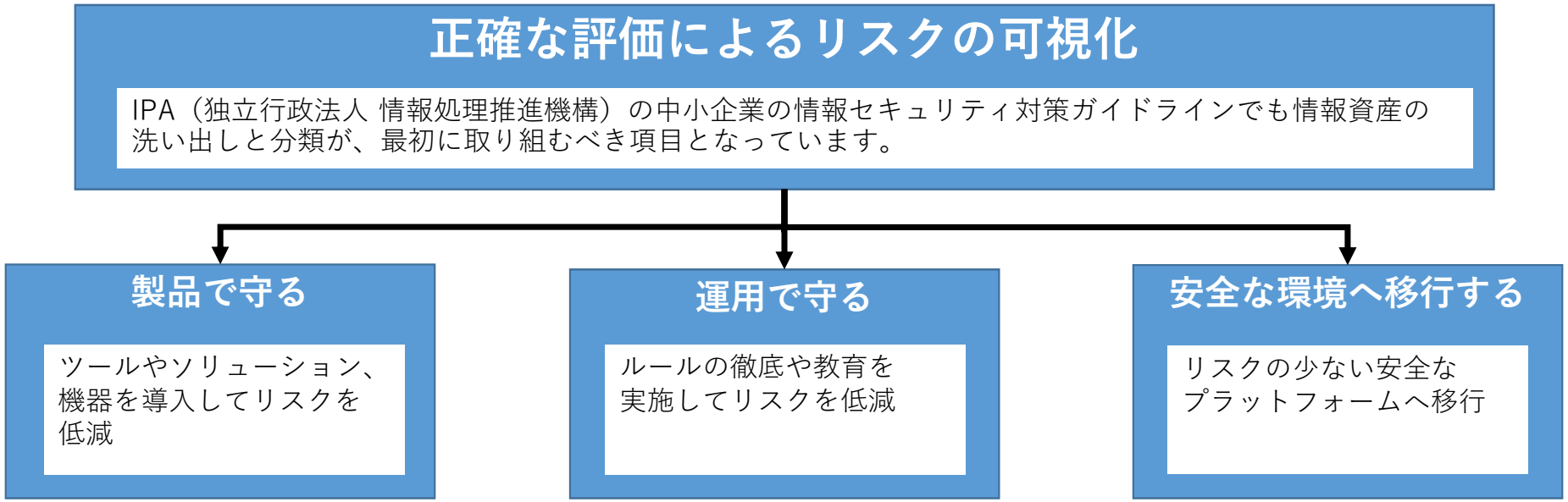
Point

営業情報という重要データが無防備なまま

正しく対策を行わなければ、限りのある予算を効果的に活用できません。

セキュリティ対策の第一歩は「情報資産の棚卸し」

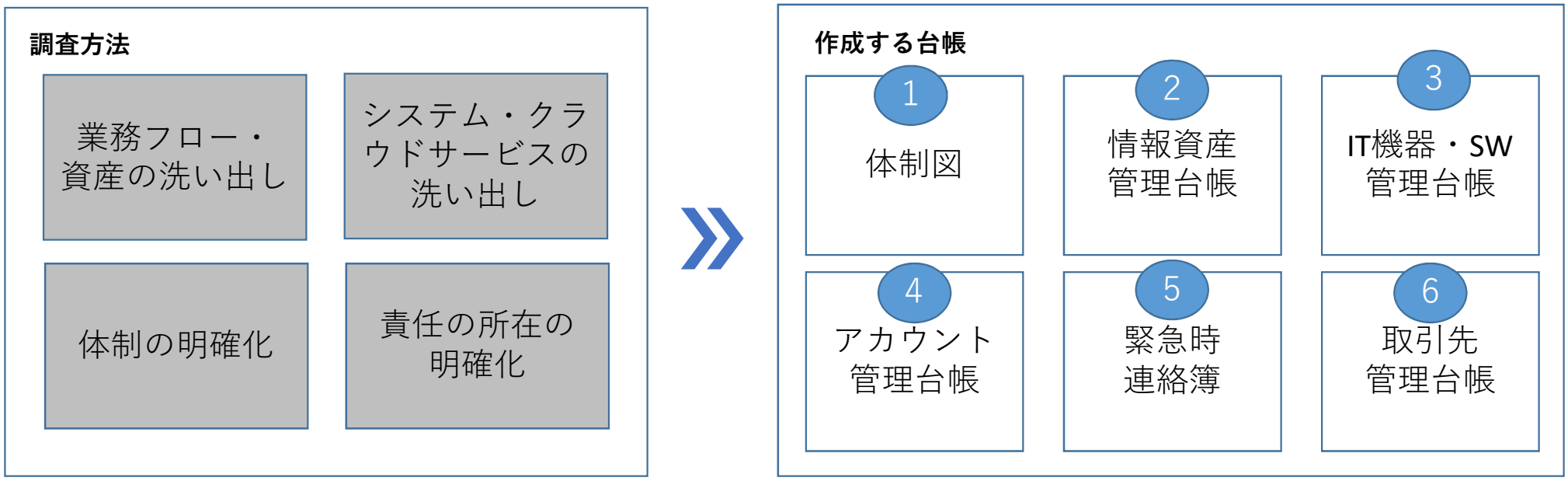
現状把握を伴わない局所的なツールの導入ではなく、まずは自社のアセスメントが確実な対策になります。
「自社に何があり、どこにリスクがあるか」を整理・把握することが、すべての対策の出発点です。



情報資産が把握できていなければ、「効果の上がらない対策」の繰り返しになりかねません。
守るべき対象が明確になれば、メリハリのあるリスク対策が可能になります。

現状の把握と必要な「6つの台帳」

守るべき情報資産と価値が分からなければリスクを可視化できません。まずは、実態を把握して次の台帳を作成します。



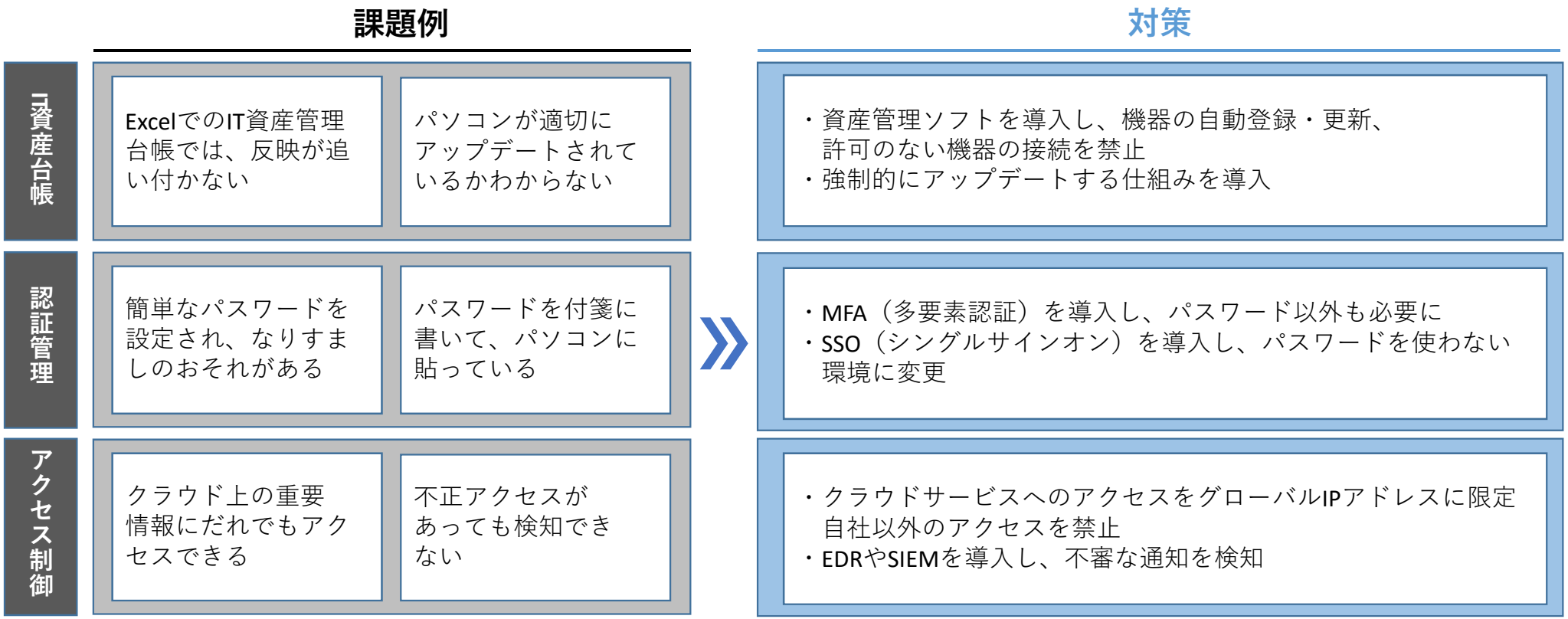
社内の情報資産台帳やIT機器台帳は作っていても、取引先管理台帳が抜け落ちているケースが多く見受けられます。

今後は取引先へ「何のデータをどのように渡しているか」の正確な把握が必要です。

これらの情報を正しく整理することで、管理すべき対象が可視化され対策を取りやすくなります。

課題の把握と対策の選定

6つの台帳を作成し、管理できていない課題に対し自社に合わせた対策を実施します。



適切なツールやソリューションで、管理工数を減らしつつも確実に管理する仕組み化が重要です。

運用と教育

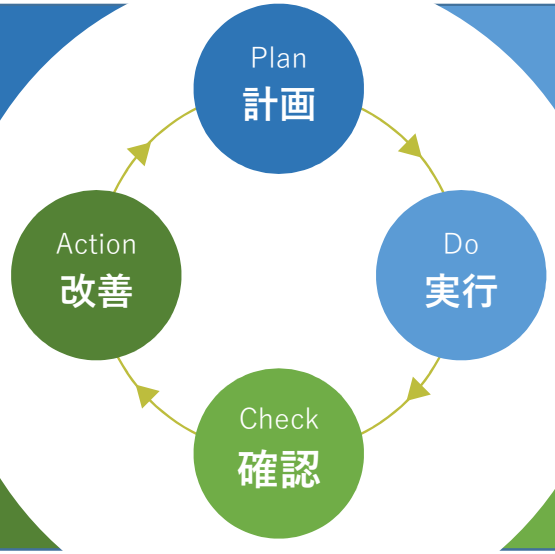
高度なシステムを導入しても、正しく運用できなければ効果が続きません。サイバー攻撃の進化に合わせた運用のアップデートと活用する人の教育が重要です。

Plan（計画）：
実態に即したルールと教育計画の策定

自社に合ったセキュリティルールを策定
誰に・どのような教育や訓練が必要かの
年間計画を立てる

Do（実行）：
実践的な訓練と報告しやすい環境づくり

実践的な訓練の実施と、ミスや違和感を
「迷わず報告できる文化」の醸成



Action（改善）：
ルールの見直しとシステムによる仕組み化

ミスしやすいルールや手順の見直し
防げないミスは、人の手に依存しないシ
ステムによる改善を実施

Check（確認）：
効果測定と潜在的リスクの可視化

実施した訓練を総合的に評価し、組織の
セキュリティ体制が正しく機能している
かを確認

SolarWinds（ソーラーウィンズ）事件

歴史上最大のサプライチェーン攻撃
アメリカ政府機関や世界の大企業数万社が導入していたIT管理ソフトのアップデートプログラムに、ウイルスが混入
ウイルスを発見したのは、MFAの登録タイミングに**違和感を抱いた担当者の直感**

ツールを入れて終わるのではなく、システムと人によるセキュリティ対策を全社で構築・運用し続けることが、組織を守るうえで重要です。

事例1：Google Workspaceへのプラットフォーム移行

度重なるシステムや機器の追加による管理コストの増加に悩んでいたクライアント様への改善事例です。サーバの保守やパッチ適用による管理工数とコスト増に対して、Google Workspaceへ移行することで大幅な経費削減とセキュリティ向上を成し遂げました。

Before

■課題

老朽化したサーバとパソコンの更新コストの高騰
脆弱性対策のパッチ適用工数が増大
突然の機器故障による予期せぬ出費
サーバの保守費用の高騰
Microsoft製品のライセンス料高騰

After

■対策

クラウドサービスのGoogle Workspaceへ移行
パソコンをChromebookへ刷新
旧システムはCameyoで仮想化

Point

捨てきれないWindows環境は仮想化で温存

導入効果

リース費用・機器保守料

5年間 ▼2000万円削減

運用工数

▼30%ダウン

★3が求める
IT資産台帳の
自動化も実現

クラウドサービスの有効活用で、コストダウンとセキュリティを両立させつつ、格付け★3をクリアする環境への移行を実現

事例2：既存環境を活かす次世代認証の構築

パスワード漏洩リスクの低減や管理コストの増大に悩んでいたクライアントの改善事例です。IDaaSと顔認証システムの導入・ActiveDirectoryとの連携により、アカウントの2重管理解消による工数削減、厳格な本人確認の実現を成し遂げました。

Before

■課題

パスワードの使い回し
退職者のアカウント消し忘れが発生
クラウドと社内システムが混在し管理工数の増大

他人になりすましアクセスできる状態

After

■対策

IDaaSでSSO構築、アカウントを一元管理
顔認証＋デバイス認証でパスワードレス化
退職時はADの操作一つで全アクセス遮断

Point

顔認証により本人以外の操作を排除。
外部だけでなく内部のなりすましも防止。
ゴーストアカウントによるリスクをゼロに。

導入効果

なりすまし防止	**ゴーストアカウントゼロ**	**管理工数の大幅削減**

本事例ではIDaaSによるアカウント管理の自動化と顔認証によるアクセス制御の強化により、★3が求めるアカウント台帳整備と不正アクセス対策の要件をクリアしています。

「外部だけでなく内部の不正アクセスにも強いゼロトラスト環境」と「確実な管理体制」を構築し、格付け★3の要件をクリアしつつ、管理工数の低減を実現

さいごに

セキュリティ対策は、ツールを入れれば終わりではありません。

現状把握から台帳整備・対策選定・運用のサイクルを回し続けることが、格付け★3をクリアする近道です。

「セキュリティ対策伴走支援サービス」では、実態にあった施策を伴走支援します。

対策選定　導入支援　運用支援　社員教育

まずは、お気軽にお問い合わせください

お問い合わせ先

サンプル株式会社

Tel：03-1234-5678

お問い合わせ：https://www.sample.com/Contact

〒100-0001 東京都千代田区1番1号　サンプルビル3F

相談・お見積りはちら

お問い合わせ

サービス概要はこちら

資料請求する