中小企業向け

セキュリティ対策レベルアップに向けた手引き

一般社団法人
日本自動車工業会

総合政策委員会　ICT部会
サイバーセキュリティ分科会

一般社団法人
日本自動車部品工業会

DX対応委員会　サイバーセキュリティ部会

2026年3月

本手引きが生まれた背景と目的

中小企業の皆様の「困りごと」に寄り添い、対策への最初の一歩を支援します

- **中小企業のための実践ガイド**
  - ✓ アンケートから、中小企業の皆様が「経営層の理解」「人材不足」「予算確保」に悩む実情が分かりました
  - ✓ 本手引きは、IT専門家でなくても、リソースが限られていても、**「自社で実践できるセキュリティ対策」**の始め方、進め方を支援する「実践的な手引き」です
- **優先項目に絞った効果的な対策**
  - ✓「自動車産業サイバーセキュリティガイドライン」には153項目ありますが、中小企業の負担軽減と実効性向上を重視し、**「優先8項目とその達成条件19件」**に絞り込みました
  - ✓ この優先項目から着実に実行することで、最小限の工数で最大のセキュリティレベルアップを目指します
- **現場の「生の声」から生まれた事例**
  - ✓ 巻末や各Stepの「他社事例」は、実際にセキュリティ対策に取り組む企業への詳細なインタビューに基づいています
  - ✓ 現場の「生の声」を反映した事例から、実践的なヒントや教訓を得る機会にしていただければと思います

Copyright© Japan Automobile Manufacturers Association, Inc.

目次

Copyright© Japan Automobile Manufacturers Association, Inc.

1．はじめに

【この章の内容】

・今、サイバーセキュリティ対策が不可欠な理由　：自動車産業でのリスクとサプライチェーン責任※を解説
・この手引きの使い方と目的　：IT専門家でなくてもできる最小限の活動とそのゴールを説明
・対策全体の3つのステップ　：守るもの、固める入口、備える事態、という流れを図解

※「サプライチェーン責任」とは、大手メーカーから部品メーカー、そのまた下のサプライヤーまで、製品の製造・供給に関わる全ての企業が、それぞれの立場で情報セキュリティを含むリスク管理を徹底する義務を指します。

Copyright© Japan Automobile Manufacturers Association, Inc.

今、サイバーセキュリティ対策が不可欠な理由①

「うちの会社は大丈夫！」その油断が、事業を脅かします

- 「大手企業向け」と思われがちなサイバー攻撃は、**今や中小企業も直接の標的**になりえます。大手企業のセキュリティ強化に伴い、攻撃者は**対策がより手薄な取引先を「侵入経路」**として狙う恐れがあるからです。貴社の事業継続のため、対策を**「自分事」**と捉え、行動を始めましょう。

中小企業も狙われるという現実

サプライチェーン攻撃の増加：
貴社が大手企業への「侵入経路」となるリスクは他人事ではありません。**取引先経由でマルウェア感染**が広がり、**サプライチェーン全体に甚大な被害**が及んだ事例が多発しています。

ランサムウェアの脅威：
貴社の機密情報や生産システムが暗号化され、**事業活動が完全に停止**した場合、**多額の復旧費用**や**賠償責任を求められる可能性があります**。

セキュリティ対策の不備は、**自社の事業継続、従業員の雇用、顧客からの信頼**を脅かす重大なリスクです。

本手引きは、この危機に対応するための「最初の一歩」をご支援します！

Copyright© Japan Automobile Manufacturers Association, Inc.

今、サイバーセキュリティ対策が不可欠な理由②

対策しないリスクは「事業停止」 会社としての信頼失墜に繋がります

- サイバー攻撃による被害は、金銭的損失だけではありません。**生産停止や情報漏洩は、貴社の「事業継続」と「将来の成長」を阻む死活問題**です。対策はもはやコストではなく、必須の投資と捉えましょう。

中小企業が直面する『対策しないリスク』

事業機会の喪失：
セキュリティ対策が遅れれば、**新規・既存取引の機会を失う**可能性があります。現在、セキュリティが取引要素の一つとして考慮されるなど、時代が変わってきています。

甚大な被害と信頼失墜：
サイバー攻撃によるシステム停止や情報漏洩は、**生産活動の停止、納期の遅延、賠償責任**など、事業継続を困難にするほどのダメージを与え、**取引先からの信頼を失墜**させます。

【ユーザー企業アンケートで明らかになった共通課題】
・多くの中小企業が**「予算確保」「人材不足」「経営層の理解醸成」**に課題を抱えています。

本手引きは、これらの課題に対し、**「IT専門家でなくてもできる最小限の活動」**で、
貴社の対策を力強く後押しします！

Copyright© Japan Automobile Manufacturers Association, Inc.

今、サイバーセキュリティ対策が不可欠な理由③

『コスト』ではない、『未来』への投資　最初の一歩を踏み出しましょう

- サイバー攻撃はいつ貴社を襲うかわかりません。セキュリティ対策への投資は、**事業、雇用、信用を守るための『未来への重要な投資』**です。この手引きは、その「最初の一歩」を支援します。

今すぐ対策を始めるべき理由

事業存続の危機：

・システム停止の被害は数千万円から数億円規模。
対策への投資は、この甚大な被害から自社を守る『保険』と考えましょう。
・「事業継続のためにはセキュリティ対策が不可欠」という**経験企業の声**は重いです。

「できること」から始める安心感：

本手引きは、「最小限のアクション」に絞り込み、
「費用ゼロでできること」や「小さな改善」から着実にセキュリティレベルを引き上げられるよう設計されています。

本手引きの「Step0」から読み始め、最初の一歩を踏み出してください。
私たち自工会・部工会とともに、貴社のセキュリティレベルを向上させましょう！

Copyright© Japan Automobile Manufacturers Association, Inc.

この手引きの使い方と目的①

総務部門が専門知識なしで推進できる「最小限の活動」を定義

- 本手引きは、ITセキュリティの専門家でなくても、総務部門の推進力で実行可能なアクションに絞り、限られた工数で最大の効果を得ることを目指します。

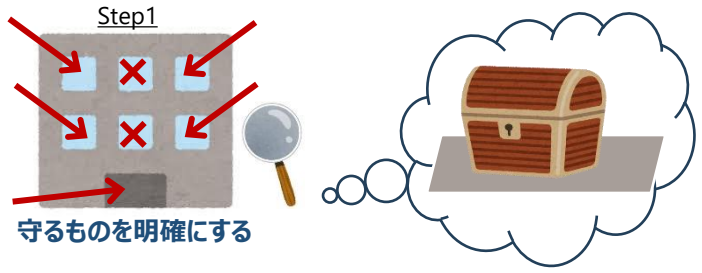
目的１

【ゴール：リスクの明確化とセキュリティ基盤の構築】

活動の最終目標を定義します：

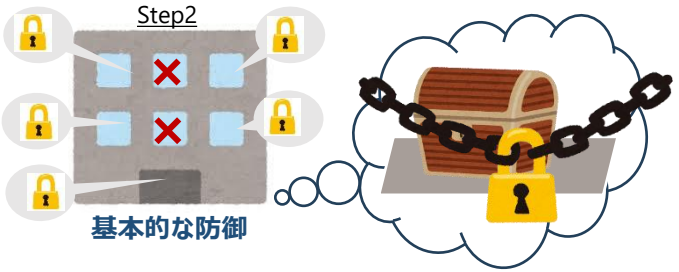
Step1：守るべき「資産」を見える化する

⇒ リスクを明確にする
（窓や扉の所在や状況を調べる）



Step2：基本的な「入口」を確実に固める

⇒基本的なセキュリティ基盤を確実に構築する
（強固な鍵をかける/新しい鍵に交換する）



Copyright© Japan Automobile Manufacturers Association, Inc.

この手引きの使い方と目的②

曖昧さを排除し、具体的に「誰が・何を・どう」すべきかに特化した手順

- 本手引きでは学術的な解説を避け、各タスクをチェックリスト形式で提示することで、具体的な活動の進め方を明確に示します。

目的２

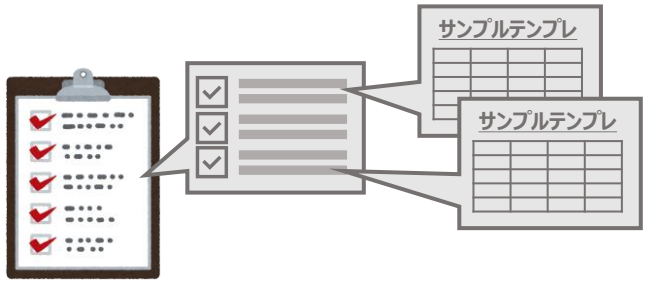
【実効性の高いチェックリストと手順に特化】

学術的な解説を避け、

- **各タスクをチェックリスト形式で提示**
- 具体的に**「誰が」「何を」「どうすべきか」**を明確に提示

曖昧なタスクや過剰な投資を避けることで、

最短ルートで防御レベルを引き上げます。



Copyright© Japan Automobile Manufacturers Association, Inc.

この手引きの使い方と目的③

有事の対応体制確立と、継続的な改善（PDCA）による自走がゴール

- 本手引きを導入時のマニュアルとして、またサンプルシートを経営層への報告資料として活用し、有事の対応体制と継続的な改善体制を確立してください。

目的３

【有事の対応体制と継続的な改善】

対策実行とは、以下の体制確立を意味します：

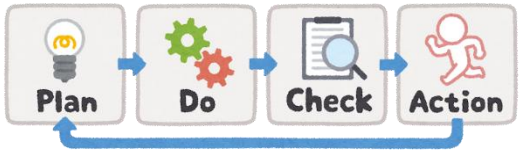
Step3：「もしも」の事態に備える

⇒事故発生時、被害を最小化する体制を確立する

もしもの事態に備える

Step1~3：PDCAサイクルを回す

⇒継続的な改善体制を確立する



Copyright© Japan Automobile Manufacturers Association, Inc.

対策全体の3つのステップ

「守るものを知り」→「入口を固め」→「もしもに備える」

- セキュリティ対策は、この論理的な3ステップで進めます。各ステップの目的を理解し、順番通りに進めることで、確実かつ効率的に防御レベルを向上させます。

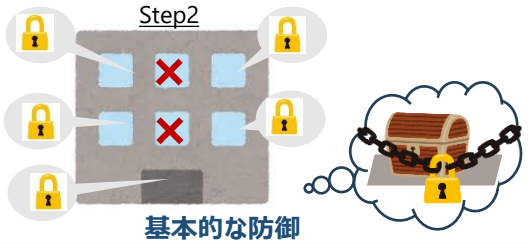
ステップ1
守るべき「資産」を見える化する

目的:
そもそも**何を守るべきか**（顧客情報、技術文書など）を明確にし、リスクの高い場所を特定します。

対応ページ: P.26~40 Step1
（情報資産リストの作成、リスク優先順位付け）

ステップ2
基本的な「入口」を確実に固める

目的:
外部からの**侵入経路として最も狙われやすい基本的な防御**（パスワード、権限、更新）を全従業員を巻き込んで確実に実行します。



対応ページ: P.41~62 Step2
（パスワード強化、アクセス権設定、ソフト更新）

ステップ3
「もしも」の事態に備える

目的:
侵入を許した場合の**被害を最小化するための備え**（バックアップ隔離、緊急連絡体制）を構築します。

対応ページ: P.63~77 Step3
（バックアップ、BCP、PDCA報告）

迅速な実行が、次のステップへの鍵となります。各ステップの完了目安を確認しながら、進めてください。

Copyright© Japan Automobile Manufacturers Association, Inc.

対策レベルアップへの道

Step0：推進のための準備と承認 と、継続活動が成功のカギ

- サイバーセキュリティ対策は、単なる技術的な課題ではありません。「組織全体で取り組むべき経営課題」として認識し、継続的に推進していくことが不可欠です。

【Step0で取り組むこと】

Step1~3の対策実行をスムーズに進めるための「**土台作り**」です。 特に、ユーザーアンケートで課題として挙げられた3点に焦点を当てます

- **経営層の理解促進と承認**
- **予算の確保と推進体制の構築**
- **脅威情報の収集**

【Step3以降も継続して行うこと】

セキュリティ対策は一度行えば終わりではありません。変化し続ける脅威に対応し、対策レベルを維持・向上させるための「**PDCAサイクル**」を回し続けることが重要です。

- **最新の脅威情報収集と共有**
- **対策状況の定期的な見直しと改善**
- **従業員への継続的な教育・啓発**
- **BCP（事業継続計画）の訓練と評価**

本手引きでご紹介する「Step1~3」の対策を実りあるものにするためには、まずStep0で強固な基盤を築き、そして「継続活動」として対策レベルを維持・向上させていく視点が欠かせません。

Copyright© Japan Automobile Manufacturers Association, Inc.

対策レベルアップに向けた全体フロー

Step0で立上げ、対策の3ステップを行うことで基礎を築き、これを継続的に改善することで対策レベルアップを目指します

- 自動車産業におけるサイバーセキュリティ対策は、一過性の取り組みではありません。「Step0：推進のための準備と承認」で強固な基盤を築き、「Step1~3」で具体的な対策を実行し、そして「継続活動」としてPDCAサイクルを回し続けることで、貴社のセキュリティレベルは着実に向上します。

P.14~23 参照　P.26~40 参照　P.41~62 参照　P.63~77 参照　P.24~25 参照

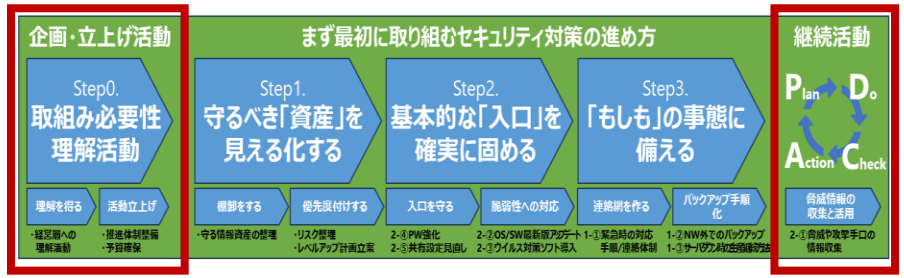
2．Step 0　推進のための準備と承認

【この章の内容】

・セキュリティを「コスト」から「信頼の基盤」へ　：「取引継続」と「復旧コスト」を経営層に提示し、行動の理解を得る

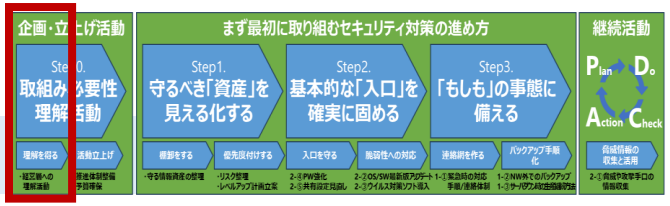
・費用ゼロから始める取り組みと推進体制　：承認を待たずに即座に実行。予算は「低コスト」から承認を得る

・脅威情報：収集と活用方法　：対策の継続に必要な最新の脅威情報の収集先と、PDCAへの活用方法を説明



Copyright© Japan Automobile Manufacturers Association, Inc.

セキュリティを「コスト」から「信頼の基盤」へ①



経営層へ訴えるべき、サイバーセキュリティの「本質」

- セキュリティ対策は、単なるコストではありません。**事業の継続と成長を支える「信頼の基盤」**への投資です。
  経営層にこの本質を理解いただくための働きかけが不可欠です。

あなたから経営層へ伝えるべき

【事業における切実な危機感と対策の価値】

経営層に対し、以下の事実を伝え、**危機感と対策の価値を共有**してください。

A社事例　B社事例　C社事例　D社事例

1.ビジネスリスク：

業界全体のサイバーセキュリティ要求の高まりに、貴社の対策が追いつかない場合、**ビジネス連携の機会を失い、競争力が低下**する可能性があります。
また、貴社が**大手企業への侵入経路として狙われる**リスクも高まり、情報漏洩やシステム停止が事業に甚大な打撃を与える恐れがあります。

対策をしない場合のリスク
- 事業機会の喪失
- 巨額の賠償責任
- 全社業務停止

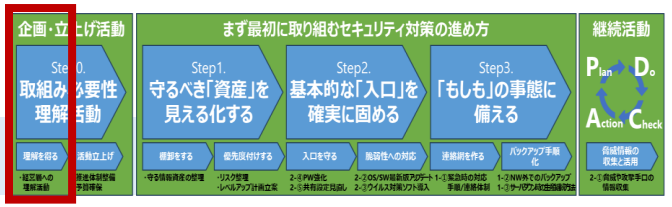
対策によるリターン（価値）
- 信頼性・ブランド向上
- 安定的な受注
- データ管理の効率化

2.対策で得られる価値：

信頼性向上：　厳しいセキュリティ基準を満たすことで、**新たなビジネスチャンス創出**につながります。
事業継続：　万一のインシデント発生時も、**迅速な復旧と事業継続**が可能となり、損害を最小限に抑えます。

Copyright© Japan Automobile Manufacturers Association, Inc.

セキュリティを「コスト」から「信頼の基盤」へ②



費用ゼロで示す、具体的な「リスクと影響額」

- 経営層の理解を得るためには、抽象的な危機感だけでなく、**具体的なリスクとその影響額を提示する**ことが効果的です。費用ゼロでできる以下の活動で、客観的な証拠を集めましょう。

経営層が動く！費用ゼロで集める

【事業に関わる具体的なリスクとその影響額の証拠】

1.リスクの可視化：

D社事例

- 情報資産の棚卸（P.27~39参照）の一部の部門で先行実施し、部分的であっても具体的にリスクを提示。
- 例）「顧客データが誰でもアクセスできる状態にあり、**情報漏えいリスク【高】**です」といった具体的な事実を提示します。

2.金額のインパクト：

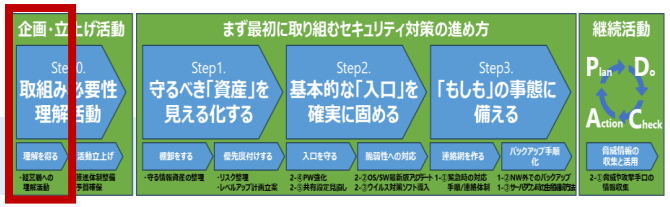
- 上記のリスク【高】のデータが暗号化された場合、
  「全従業員の3日間の業務停止（人件費・機会損失）は、〇〇万円に相当する」と概算を提示します。

※参考情報

- ランサムウェア被害の平均復旧コストは約2.5億円。（IPA「情報セキュリティ10大脅威 2024」より）
- 生産停止1時間あたりの損失額を業界平均から算出し、**「もし貴社が1日業務停止したら、〇〇万円の損失が発生する」**と具体的に伝える。

Copyright© Japan Automobile Manufacturers Association, Inc.

セキュリティを「コスト」から「信頼の基盤」へ③



対策推進で実現する「未来の価値」

- サイバーセキュリティ対策は、防御だけでなく、**貴社の企業価値を向上させ、持続的な成長を可能にする**ものです。具体的なメリットを提示し、投資への理解を深めましょう。

経営層が納得する！伝えるべき

【サイバーセキュリティ対策で得られる事業における価値】

B社事例

1.市場競争力の強化：

厳格なセキュリティ基準への適合は、**顧客や取引先からの高い信頼を獲得し、他社との差別化**を図ります。これにより、**新たなビジネスチャンス創出**につながり、市場での優位性を確立します。

2.業務効率の向上：

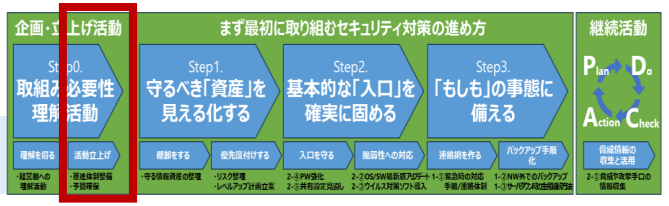
情報資産の棚卸やアクセス権限の整理（P.46~50参照）を通じて、**情報の所在と管理が明確化**されます。これにより、**従業員の「探す時間」が削減**され、業務プロセス全体の効率化が図れます。

3.戦略的経営判断の支援：

守るべき情報資産とそれに含まれるリスクが客観的に把握されることで、**経営層はリスクに基づいた適切な意思決定**を下し、事業戦略にサイバーセキュリティを組み込むことが可能になります。これは、事業の安定と成長に不可欠な要素です。

Copyright© Japan Automobile Manufacturers Association, Inc.

費用ゼロから始める取り組みと推進体制①



まずは現状把握から　社内の「PC好き人材」を巻き込んだ協力体制の構築

- この手引きを活用し、まずは貴社全体のセキュリティ状況を自ら把握することから始め、社内の「PC好きの人材」に協力を仰ぎましょう。

【セキュリティ推進リーダーとしての第一歩】

現状把握の着手：
この手引きを活用し、まずは**貴社全体の情報セキュリティ状況**（例：情報資産の棚卸など）を**自ら把握**することから始めます。

社内の「PC好き人材」との連携：
社内でPCやネットワークに詳しい**「PC好きの人材」**を見つけ、彼らに協力を仰ぎましょう。IT専門部署がなくても、既存の人材（総務や製造部門の担当者など）に役割分担を相談し、**「仲間」として協力体制**を築きます。

小さな成功体験の積み重ね：
費用ゼロで実施可能な対策（例：情報資産の棚卸、不要なアクセス権限の削除など）から着手し、その成果を報告することで、周囲に**「着実に進めている」という安心感**を与え、協力者を増やします。

【事例に学ぶ：社内の「PC好き人材」の発掘と活用】

具体的な取り組み： A社事例

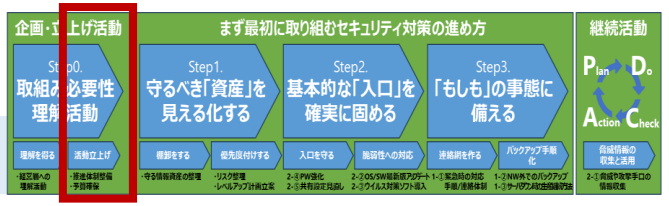
A社では、情報システム部門がない中、**PCやネットワークに詳しい総務部の担当者を推進リーダーに指名**。彼が社内の「PC好き人材」に声をかけ、**情報交換会を定期開催**。これにより、非公式ながらも協力体制が生まれ、担当者がベンダーへの相談内容を具体化できた。

得られた教訓：

既存の人材の得意分野を活かし、情報共有の場を設けることで、専門部署がなくとも効果的な推進体制を構築できる。

Copyright© Japan Automobile Manufacturers Association, Inc.

費用ゼロから始める取り組みと推進体制②



各部署のキーマンを味方に　経営層の後押しによる組織的な推進力の強化

- 各部署の業務内容を深く理解しているキーマンに、セキュリティ対策の重要性を伝え、協力を依頼すると共に、経営層からの公式なメッセージで組織的な推進力を高めます。

【部門連係による協力体制の構築】

各部署のキーマンを味方に：
各部署の**業務内容を深く理解しているキーマン**に、セキュリティ対策の重要性を伝え、協力を依頼しましょう。

部門責任者の巻き込み：
各部門の責任者をセキュリティ推進の担当者と位置づけ、それぞれの部署での**対策実行を促す役割を明確に**することが、**組織的な推進力**を高めます。

経営層からの後押し：
経営層からの「セキュリティ責任者の言うことを聞くように」といった**メッセージ**は、セキュリティ推進を公的に後押しし、部門連携を円滑にします。

【事例に学ぶ：経営層の後押しで部門連携を強化】

具体的な取り組み： B社事例

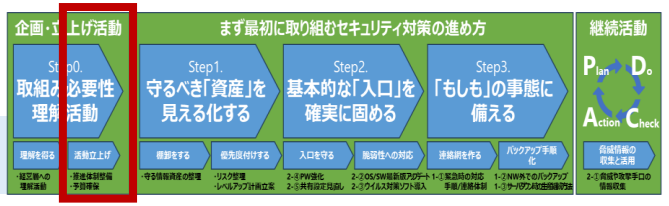
B社では、**経営層が定期的な朝礼**で「各部署はセキュリティ推進担当者の指示に従うように」と**繰り返し発信**。これにより、各部門の責任者が積極的に協力するようになり、スムーズな部門連携が実現した。

さらに、協力に難色を示す部門長が率いる部門への突破口として、**内部のキーマンを味方につけて、部門内部を巻き込んだ**ことで、部門連携の推進を実現した。

得られた教訓：
経営層からの明確なメッセージは、組織全体のセキュリティ意識を高め、部門間の連携を促進する上で大きな推進力となる。

Copyright© Japan Automobile Manufacturers Association, Inc.

費用ゼロから始める取り組みと推進体制③



身近な機器の状況把握による、自社の潜在リスクと被害想定額の可視化

- 「情報資産棚卸ワークシート」を用いてガイドラインの観点で対応状況を確認し、自社にとって重要かつリスクの高い箇所を特定してください。

【費用ゼロで集める「リスクと金額の証拠」】

情報資産の棚卸（P.27~39参照）を先行実施：

まずはStep1で推奨される情報資産の**棚卸を先行して実施**します。
「データ/機器資産棚卸ワークシート」を用いて「自動車産業サイバーセキュリティガイドライン」の観点で対応状況を確認し、重要度と合わせて**高リスク箇所を特定**します。

リスク顕在化時の「影響額」を試算：

洗い出した**リスクが顕在化した場合の具体的な被害額を試算**します。
- 「顧客データの情報漏えいが発生した場合、賠償金やブランド毀損で〇〇万円の損失」
- 「生産管理システムが停止した場合、1日あたり〇〇万円の機会損失」など

自社にとって**最もインパクトの大きいシナリオに焦点を当てます**。ランサムウェア被害の平均復旧コストや、生産停止による損失額の業界平均などを参考に**概算を算出**します（P.16参照）

【事例に学ぶ：具体的な被害額を試算して経営層を説得】

具体的な取り組み：D社事例

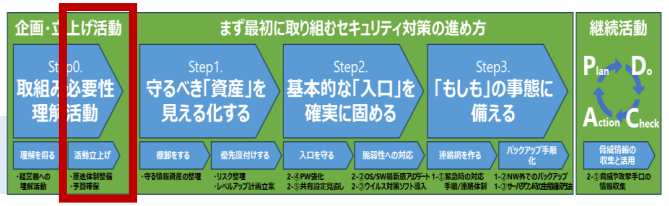
D社では、**過去のサイバー攻撃被害経験**から、情報資産の棚卸を実施し、**どのデータが暗号化されたら、どれだけの期間業務が停止し、その結果いくらの損失**（機会損失、復旧費用、信用低下）が発生するかを**具体的に試算**。その資料を経営会議で提示したことで、新たなセキュリティ対策予算の獲得に成功した。

得られた教訓：

抽象的な「危ない」ではなく、**具体的な「金額」でリスクを伝える**ことが、経営層の意思決定を促す。

Copyright© Japan Automobile Manufacturers Association, Inc.

費用ゼロから始める取り組みと推進体制④



費用ゼロの改善から着手　小さな成功実績の積み重ねによる予算確保へ

- 費用ゼロで実施可能な対策から着手して具体的な改善効果を創出し、小さな成功体験を定期的に経営層へ報告して信頼と予算の確保に繋げてください。

【信頼を獲得する「行動と報告」】

「できること」から着手し成果を出す：

費用ゼロで実施可能な対策から着手し、具体的な改善効果を創出します。

これらの**小さな成功体験を定期的に経営層に報告**することで、「着実に進めている」という**安心感と信頼を獲得**し、その後の予算確保に繋げます。

報告資料としての活用：

棚卸結果やリスク分析、試算した被害額は、経営層への報告資料としてそのまま活用できます。**客観的なデータに基づいた報告**は、理解と承認を得る上で強力な武器となります。

【事例に学ぶ：小さな改善から信頼を構築】

具体的な取り組み：B社事例

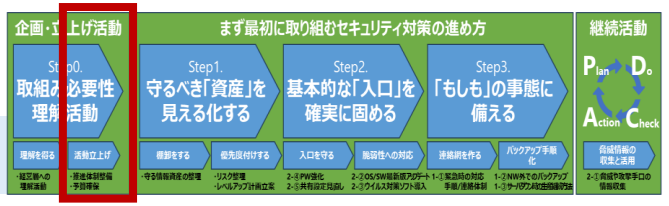
B社では、まず**費用ゼロで実行可能**なパスワードポリシーの強化とアクセス権限の棚卸を実施。**改善前後の状況**（例：パスワードの複雑性向上、Everyone権限の削除）を**数値で報告**し、経営層に「目に見える成果」を提示。これにより、さらなる対策への予算確保への道筋をつけた。

得られた教訓：

まずは費用をかけずに**できることから着手**し、その成果を報告することで、**経営層からの信頼**を得て、長期的な支援体制を築く。

Copyright© Japan Automobile Manufacturers Association, Inc.

費用ゼロから始める取り組みと推進体制⑤



「事業継続」や「信用維持」など、経営課題としての対策の必要性を訴求

- 「事業継続」、「サプライチェーン責任」や「競争力強化」など、経営層が最も重視する事業上の視点から、対策がコストではなく未来への投資であることを訴求します。

【経営層の関心領域で訴求するポイント】

事業継続と社会的信用：

事業への直接的な影響を伝えます。

「サイバー攻撃により生産ラインが停止すれば、**納期遅延や取引停止**に繋がり、事業継続が困難になる」「情報漏えいは、**顧客や取引先からの信用を失い**、ブランド価値を大きく損なう」

コスト削減と競争力強化：

長期的な視点でのメリットを強調します。

「予防的対策への投資は、インシデント発生後の**莫大な復旧コスト**(P.16参照)を回避できる」
「セキュリティ基準への適合は、**新たなビジネスチャンス創出や取引先からの信頼獲得**に繋がり、市場での競争力を高める」

従業員と企業の資産保護：

会社全体へのメリットを明確にします。

「強固なセキュリティは、**従業員が安心して働ける環境を守り**、大切な技術ノウハウや企業秘密といった**資産をサイバー脅威から守るための投資**である」

【事例に学ぶ：「生産停止」のリスクを可視化して危機感を共有】

具体的な取り組み：D社事例

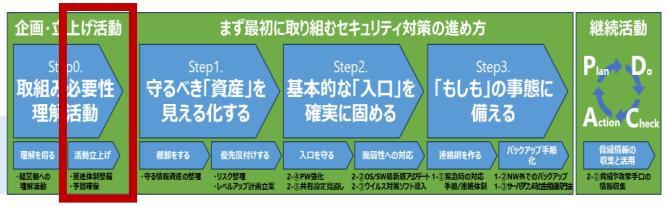
D社では、実際にサイバー攻撃を経験した際に、経営層に対し**「生産停止が続けば、取引先への賠償責任やビジネス機会の損失に繋がり、最悪の場合、会社の存続が危うくなる」と具体的に説明**。
この経験から、経営層はセキュリティ対策を最重要課題と認識するに至った。

得られた教訓：

経営層が最も避けたい**「事業の根幹に関わるリスク」**を明確に伝え、当事者意識を持たせることが重要。

Copyright© Japan Automobile Manufacturers Association, Inc.

費用ゼロから始める取り組みと推進体制⑥



他社事例による危機感の共有と、定期報告による長期的な支援体制の確立

- 改善の実績や、同業他社の被害事例を定期的に簡潔に報告し、経営層に「明日は我が身」という当事者意識を持たせ、長期的な支援を取り付けてください。

【効果的なコミュニケーションの実践】

具体的な事例で危機感を醸成：
同業他社やサプライチェーン企業の**サイバー攻撃被害事例**（ランサムウェア感染、情報漏えいなど）**を具体的に紹介**し、**「明日は我が身」**という当事者意識を持たせます。

定期的な「小さな成功」の報告：
Step1の棚卸結果や、費用ゼロで改善できた項目（例：脆弱なパスワードの排除、不要なアクセス権限の削除など）を**定期的に、かつ簡潔に報告**します。
具体的な進捗は、継続的な支援を得る上で非常に重要です。

【事例に学ぶ：「従業員を守る」視点で共感を獲得】

具体的な取り組み： B社事例

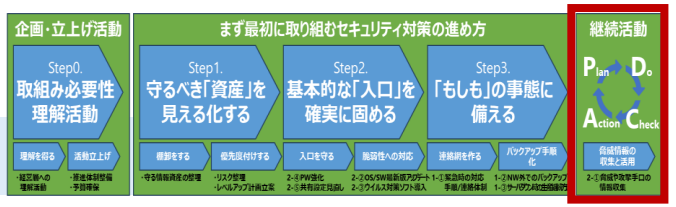
B社では、経営層への説明で「セキュリティ対策は、**従業員が安心して業務に取り組める環境を守るための不可欠な投資**である」と訴求。また、「万が一、会社の情報が漏えいした場合、**従業員にも責任が及ぶ**可能性がある」という視点も提示し、共感を得て予算を獲得した。

得られた教訓：

会社と従業員、双方のメリットを強調することで、経営層の理解と支援を得やすくなる。

Copyright© Japan Automobile Manufacturers Association, Inc.

脅威情報：収集と活用方法①



進化する攻撃への備え　IPA等の信頼できる情報源を週1回確認する習慣

- 最新の脆弱性や攻撃トレンドを把握するため、信頼できる情報源（IPA、業界団体等）を特定し、週に一度はチェックする体制を組みます。

A社事例　D社事例

【収集源の特定と登録】

信頼できる情報源を特定し、
週に一度はチェックする体制を組みます。
特に以下の情報源は、対策に直結します。

■**IPA（情報処理推進機構）の注意喚起メール：**
⇒ 国内の最新の脆弱性情報や攻撃トレンド

■**セキュリティベンダーのニュースレター：**
⇒導入済みソフトの脆弱性情報や推奨設定

■**業界団体からの通知：**
⇒自動車サプライチェーン特有の要求事項や事例

【事例】

■**IPA（情報処理推進機構）の注意喚起メール**
重要なセキュリティ情報や脆弱性情報、注意喚起が掲載されています　https://www.ipa.go.jp/security/security-alert/index.html

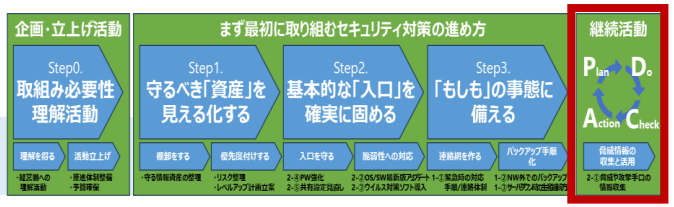
■**セキュリティベンダーのニュースレター**
最新動向など、ニュースレターや配信登録により収集することができます　ニュースレター 一覧 | トレンドマイクロ (JP)

■**自動車産業セキュリティ活動の情報提供への登録**
日本自動車工業会(JAMA)及び日本自動車部品工業会(JAPIA)が発信する各種セキュリティ活動の情報を受信できます
https://forms.office.com/r/VfU8uU5ZXx

※当スライド内のリンクは、2026年3月31日現在のもの

Copyright© Japan Automobile Manufacturers Association, Inc.

脅威情報：収集と活用方法②



得た情報を「知識」で終わらせず、社内ルールや対策の迅速な改善に反映

- 収集した情報を単なる知識で終わらせず、社内ルールの見直しやソフトウェア更新の緊急度判定など、具体的なアクションに必ず繋げてください。

A社事例 D社事例

【ルール見直しの頻度】

収集した情報に基づき、最低でも**半期に一度**は、Step2（基本対策）で定めたルールや手順書（特にパスワードルール、アクセス権限リスト）が現状に合っているか、推進チームが中心となって見直しを行います。

【脅威情報の活用：PDCAの「Plan」に接続】

得られた情報が、単なる知識で終わらないよう、必ずアクションに繋げます。

■ **脆弱性情報**
⇒ソフトウェア更新の緊急度の見直し。

■ **新しい攻撃手法**
⇒緊急連絡フロー（P.65）や従業員教育内容の見直し。

この情報収集と活用こそが、セキュリティ対策を「継続的な文化」にするためのエンジンです。

Copyright© Japan Automobile Manufacturers Association, Inc.

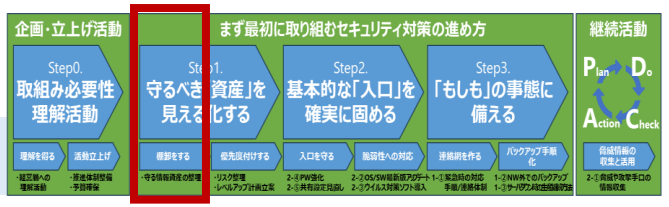
3．Step 1 守るべき「資産」を見える化する

【この章の内容】

・「情報資産の棚卸」とは何か	：守るべき情報と、それが存在する機器の洗い出し方を解説
・守るべき情報資産の分類	：情報を「機密性」で分類し、どのレベルか明確にする
・データ資産棚卸ワークシート	：情報そのものを特定・整理するためのワークシートを解説
・機器資産棚卸ワークシート	：データ資産を保管・処理する物理的な機器を特定・整理するためのワークシートを解説
・リスクの定義と評価の基本	：情報資産が持つリスクを「高・中・低」で評価する手順
・弱い場所の特定と優先付け	：現状の対策状況からリスクを評価し、強化順を決める手順
・対策項目のマッピングと担当者	：弱い場所に対し、どのステップの対策を行うか担当者を決める
・Step1の完了と次のアクション	：資産の棚卸と優先付けを完了するためのチェックリスト

Copyright© Japan Automobile Manufacturers Association, Inc.

【情報資産の棚卸】とは何か



対策の羅針盤を作る 「何を守るべきか」を明確にする最初の作業

- セキュリティ対策は、まず守るべき情報と機器（情報資産）を明確にすることから始まります。本ステップは、リスクを正しく評価し、後の対策の優先順位を決めるための土台です。

情報資産の定義

情報資産とは：
企業活動に価値を持つデータとその入れ物（機器）
具体的には、**データ**（顧客リスト、技術情報、経営計画、メール）と、データを保管・処理する**機器**（PC、サーバー、スマートフォン、紙媒体）の二つに分けて棚卸します。

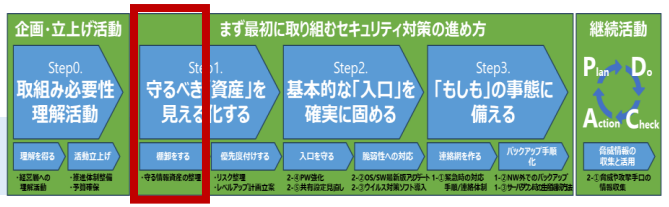
棚卸の目的

最大の目的は、**対策の優先順位付け**です。 C社事例
資産の重要度と現在の対策状況を把握し、
「最もリスクが高く、緊急に対策が必要な場所」（P.35~36）を客観的に特定します。

本ステップの成果物は、貴社のセキュリティ活動のすべてを決定づける「棚卸リスト」です。

Copyright© Japan Automobile Manufacturers Association, Inc.

情報資産の棚卸の進め方



対策の優先順位付けを行うため、棚卸を行う

- 以下の進め方に従って、情報資産の棚卸を行います。詳細は各頁を参照してください。

保有資産調査（データ資産）

データ資産について既存保有資産を調査し、**「データ資産棚卸ワークシート」**の左半分（P.30参照）を用いて、棚卸を行う
・各データ資産の重要度を分類する（P.30参照）
・保存場所は、「機器資産棚卸ワークシート」とリンクが取れるようにする

保有資産調査（機器資産）

機器資産について既存保有資産を調査し、**「機器資産棚卸ワークシート」**の左半分（P.32参照）を用いて棚卸を行う
・機器資産ごとに保存されているデータ資産を調査する（P.32参照）
・機器資産に保存されているデータ資産については、「データ資産棚卸ワークシート」とリンクが取れるようにする

対策状況の判定

「データ資産棚卸ワークシート」および、**「機器資産棚卸ワークシート」**の各情報資産について、
シート右半分の横軸のチェック観点を基に対策状況を判定し、判定理由を記入する（P.31、P.33参照）

リスク評価の判定

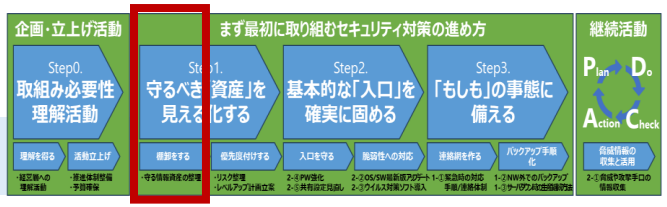
「データ資産棚卸ワークシート」および、**「機器資産棚卸ワークシート」**から、各情報資産の重要度と一番低い対策状況から
リスク判定を行い（P.35~36参照）、ワークシートの右端のリスク評価結果（A~C）を記載する（P.31、P.33参照）

対策項目のマッピング

リスク評価結果がA（最優先・即時対応）の資産を**各「資産棚卸ワークシート」**から**「実行マッピングテーブル」**へ転記し、
対策と実行責任者を紐づける（P.37~39参照）

Copyright© Japan Automobile Manufacturers Association, Inc.

守るべき情報資産の分類（重要度の決定）



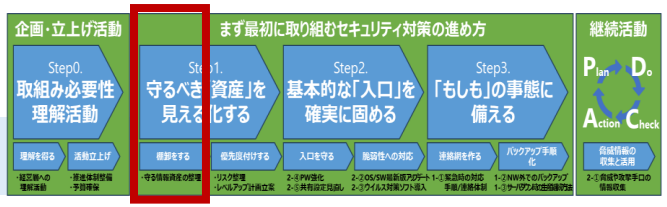
すべての情報を同じレベルで守るのは非効率　漏洩時の「影響度」で分類する

- 資産を重要度に応じて分類することで、限られたリソース（予算・時間）を最も守るべき情報に集中させることができます。以下の4段階で分類してください。

機密区分（重要度レベル）	説明	例
機密レベル 高 (極秘)	漏洩した場合、会社や取引先に極めて甚大な損害を与える情報	次期製品の設計図、試作データ、未公開の経営戦略、M&A情報、顧客の決済情報、個人を特定できる従業員情報
機密レベル 中 (社外秘)	漏洩した場合、会社や取引先の事業活動に支障をきたす可能性のある情報	財務諸表、人事評価情報、顧客名簿（連絡先のみ）、一般の設計・製造関連文書、営業戦略、社外発表前のプレスリリース
機密レベル 低 (取扱注意)	漏洩しても、会社や取引先への影響が軽微な情報	一般的な業務マニュアル、社内会議議事録、特定の部署内でのみ共有される資料、公開前の社内報
機密レベル なし (公開可)	外部に公開することを前提とした情報	Webサイトの情報、公開済みプレスリリース、製品カタログ、求人情報

Copyright© Japan Automobile Manufacturers Association, Inc.

データ資産棚卸ワークシート①



全部門の重要なデータ資産を網羅　名称・保存場所・重要度の明確化

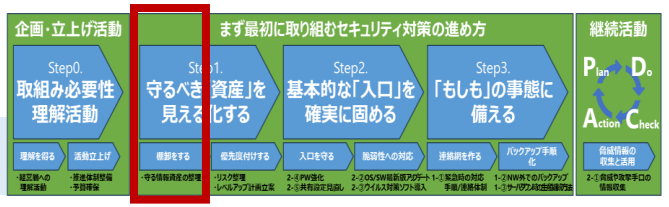
- 情報そのもの（ファイル、データベースなど）を特定するためのワークシートです。左半分には、部門ごとに、作成・保管している重要なデータ資産を漏れなく記入してください。

データ資産棚卸ワークシートの例（左半分）

No.	資産名称	管理責任部署	保存場所	重要度	バックアップ状況	・・・（右半分へ続く）
1	顧客マスターリスト (最新版)	営業部	ファイルサーバー/ 営業共通F	高	日次バックアップあり	・・・
2	R7年度 新規技術開発計画	開発部	専用サーバー/極秘F	高	週次バックアップあり	・・・
3	社員人事評価データ	総務部	総務部共有フォルダ	中	外部HDDに月次	・・・
4	R6年度 備品購入履歴	総務部	総務部共有フォルダ	低	なし	・・・
5	経理会計データ (過去3年)	経理部	専用データベース (DB)	高	ネットワーク未隔離のDB サーバー	・・・

Copyright© Japan Automobile Manufacturers Association, Inc.

データ資産棚卸ワークシート②



ガイドラインに基づき、各資産の対策状況とリスクレベルを客観的に評価

- 各データ資産に対し、「自動車産業サイバーセキュリティガイドライン」の**優先的に取り組むべき優先項目と、関連項目No. の達成度合い**を調査し、調査結果から資産に対するリスク評価を行います。

データ資産棚卸ワークシートの例（右半分）

No.	資産名称	…	重要度	…	1-②バックアップ		…	リスク評価結果
					No. 148　適切なタイミングでバックアップできている	No. 149　復元（リストア）手順を整備している	…	
1	顧客マスターリスト(最新版)	…	高	…	**対応十分**：毎日0:00~05:00にバックアップを実行	**対応不十分**：手順書があるが、最新のシステム構成と乖離	…	リスクレベル【A】
2	R7年度 新規技術開発計画	…	高	…	**対応十分**：バックアップを実行	**対応十分**：手順書あり	…	リスクレベル【C】
3	社員人事評価データ	…	中	…	**対応十分**：月次で外部HDDへバックアップを実行	**対応不十分**：復元手順なし	…	リスクレベル【B】
4	R6年度 備品購入履歴	…	低	…	**対応不十分**：バックアップなし	**対応不十分**：復元手順なし	…	リスクレベル【C】
5	経理会計データ(過去3年)	…	高	…	**対応不十分**：バックアップなし	**対応不十分**：復元手順なし	…	リスクレベル【A】

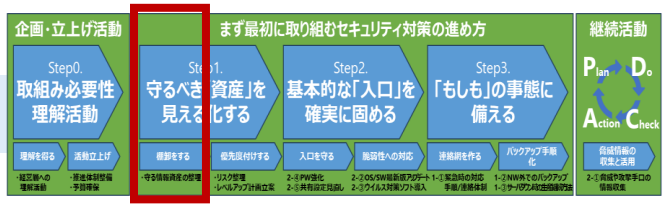
作成手順

1. チェック観点を基に対策状況を判定し、判定理由を記入する
2. 各資産の重要度と一番低い対策状況からリスク判定を行い（P.35~36参照）、リスク評価結果（A~C）を記載する
3. リスクレベルがA（最優先・即時対応）の資産を「実行マッピングテーブル」（P. 39参照）へ転記し、対策と実行責任者を紐づける

このリストが、Step2以降で「何を、どれだけ厳しく守るか」を決定します。

Copyright© Japan Automobile Manufacturers Association, Inc.

機器資産棚卸ワークシート①



PC・サーバー管理状況を網羅し、守るべき「入れ物」を特定

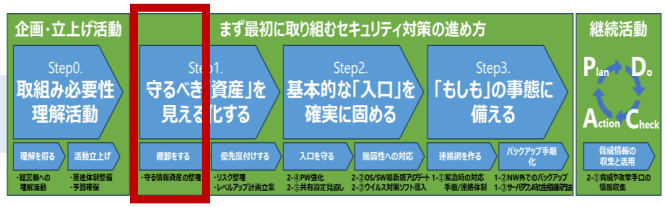
- データ資産を保管・処理するPC、サーバー、スマホ等のハードウェアを特定し、特にインターネット接続されている機器を優先的にリスト化してください。

機器資産棚卸ワークシートの例

No.	機器名称/管理番号	設置場所/使用者	OSの種類とバージョン	対策ソフト名/更新状況	外部接続状況	保管データ（重要度）	・・・（右半分へ続く）
1	ファイルサーバー #01	サーバールーム	Windows Server 2019	EDR製品 / 最新	常に接続	顧客データ（高） 会社共有データ（高）	・・・
2	営業部 PC-005	営業部 / 山田	Windows 10 Pro 21H2	OOOアンチウイルス / 期限切れ	常に接続	個人データ（高）	・・・
3	経理部 PC-002	経理部 / 田中	Windows 11 Pro	OOOアンチウイルス / 最新	常に接続	取引データ（高） 顧客データ（高）	・・・
4	予備機 PC-012	倉庫	Windows 7	なし	ネットワーク切断	取引データ（高） 顧客データ（高）	・・・
5	開発用タブレット	開発部 / 鈴木	Android 12	なし	Wi-Fi接続	技術資料（低）	・・・

Copyright© Japan Automobile Manufacturers Association, Inc.

機器資産棚卸ワークシート②



機器ごとの対策状況を確認し、ガイドラインに基づくリスク評価を実施

- 各機器に対し、事故発生時の対応体制や責任者が明確になっているか等の対策状況を判定し、改善が必要な端末を浮き彫りにします。

機器資産棚卸ワークシートの例

No.	機器名称/管理番号	…	保管データ（重要度）	…	1-①連絡体制		…	…	リスク評価結果
					No.18　情報セキュリティ事件・事故発生時の対応体制とその責任者を明確にしていること	No.20　定期的、または必要に応じて事故の体制を見直ししている	…		
1	ファイルサーバー #01	…	顧客データ（高） 会社共有データ（高）	…	**対策十分**：情報システム部門が中心となって整備済み	**対策十分**：過去事例、新たな脅威を随時対策済み		…	**リスクレベル【C】**
2	営業部 PC-005	…	個人データ（高）	…	**対策不十分**：紛失時の初動対応の周知不足	**対策十分**：営業活動の変化に合わせて随時見直し		…	**リスクレベル【A】**
3	経理部 PC-002	…	取引データ（高） 顧客データ（高）	…	**対策十分**：機密情報を扱うため、詳細に整備済み	**対策十分**：外部環境の変化に合わせて随時見直し		…	**リスクレベル【C】**
4	予備機 PC-012	…	取引データ（高） 顧客データ（高）	…	**対策十分**：情報システム部が管理、整備済み	**対策不十分**：本運用機ほど見直されていない。		…	**リスクレベル【A】**
5	開発用タブレット	…	技術資料（低）	…	**対策不十分**：初動対応が個人にゆだねられている	**対策十分**：ツールに合わせた対策など随時見直し		…	**リスクレベル【C】**

作成手順

1. チェック観点を基に対策状況を判定し、判定理由を記入する
2. 各資産の重要度と一番低い対策状況からリスク判定を行い（P. 35~36参照）、リスク評価結果（A~C）を記載する
3. リスクレベルがA（最優先・即時対応）の資産を「実行マッピングテーブル」（P. 39参照）へ転記し、対策と実行責任者を紐づける

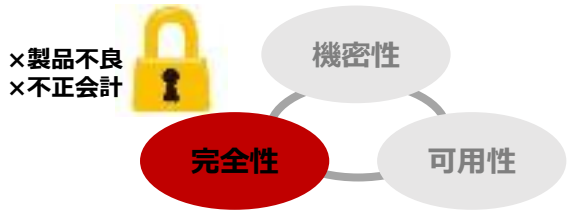
Copyright© Japan Automobile Manufacturers Association, Inc.

【コラム】リスクの定義と評価の基本

「機密性」「完全性」「可用性」の3軸で、侵害された場合の被害を見積もる

- 「リスク」とは、脅威(攻撃)によって脆弱性(弱点)が突かれ、資産が侵害される可能性です。機密性など、被害の性質を以下の3つの観点で評価し重要度を決定します。

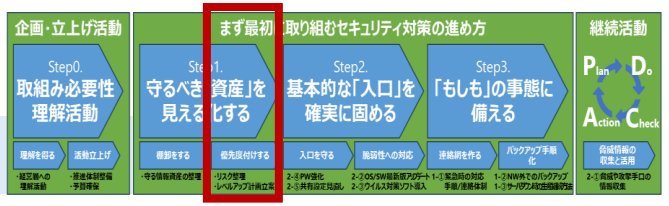
【機密性 (Confidentiality)】	【完全性 (Integrity)】	【可用性 (Availability)】
定義: 情報が外部に漏洩しないこと **被害：** 顧客情報、技術情報の漏洩による **信用の失墜、賠償問題**	**定義:** 情報が不正に改ざん・破壊されないこと **被害：** 経理データや設計図の改ざんによる **製品不良、不正会計**	**定義:** 必要な時に情報システムが利用可能であること **被害：** サーバーダウンやシステム障害による **業務停止**



本格的なリスク分析では、これら3つの観点を合わせた重要度で、各資産が侵害された場合の影響度を評価します。

Copyright© Japan Automobile Manufacturers Association, Inc.

弱い場所の特定と優先付け①



重要度と対策状況を掛け合わせ、直ちに対策が必要な「弱い場所」を特定

- 棚卸した各資産・機器に対し、現在の対策が十分かを評価してください。対策不十分な箇所を「脆弱性が高い」と判断し、リスクを特定します。

【対策状況の評価（脆弱性評価）】

データ資産/機器資産棚卸ワークシート（P.30~33）の各資産・機器に対し、現在の対策が十分かを評価します。
「対策が不十分＝脆弱性が高い」と判断します。
評価例:パスワード設定が不十分、アクセス権限が甘い、OSが古いなど。

リスクレベル決定マトリクスの例

資産の重要度＼対策状況	十分	部分的	不十分
高	C	B	A
中	C	C	B
低	C	C	C

Copyright© Japan Automobile Manufacturers Association, Inc.

弱い場所の特定と優先付け②

特定したリスク最大（レベルA）の資産へリソースを集中させ、即座に対策

- 重要度と対策状況を掛け合わせ、緊急に対策が必要な「リスクA」の資産を決定し、Step2の具体的な対策を集中して実行する準備を整えます。

【リスクレベルの決定】

「重要度」と「対策状況」を掛け合わせ、以下の優先度を決定します。

1. リスク【A】（最優先・即時対応）
重要度「高」で、かつ対策状況が「不十分」な資産。緊急に対策が必要です。

2. リスク【B】（中期対応）
重要度「高」で対策が部分的な資産、または重要度「中」で対策が不十分な資産。

3. リスク【C】（対応不要）
リスクA・B以外の資産。

この優先度【A】に絞り、Step2の対策を集中して実行します。

Copyright© Japan Automobile Manufacturers Association, Inc.

対策項目のマッピングと担当者①

最優先資産（リスクA）のみを抽出　対策の全体像を把握する一覧の作成

- 特定したリスクAの資産のみを抽出し、対策の全体像を俯瞰して管理するための「実行マッピングテーブル」を準備してください。

実行マッピングテーブルの例

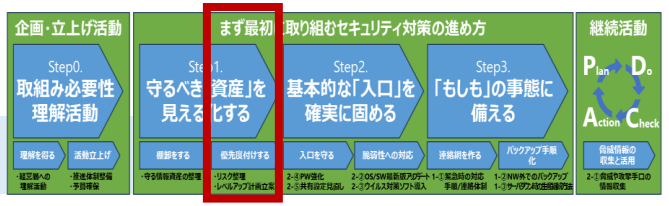
No.	資産名称 (P.30/32)	リスクレベル	弱点（脆弱性）の具体的な内容	対応すべき対策項目	実行責任者	完了期限（目標）
A-1	顧客マスターリスト (データ)	A (最優先)				
A-2	営業部 PC-005 (機器)	A (最優先)				
A-3	経理会計データ (データ)	A (最優先)				
A-4	予備機 PC-012 (機器)	A (最優先)				

マッピング手順

1. 「データ資産棚卸ワークシート」および「機器資産棚卸ワークシート」から**リスク【A】**の資産を抽出する。

Copyright© Japan Automobile Manufacturers Association, Inc.

対策項目のマッピングと担当者②



各資産の弱点に対し、Step2/3の具体的な対策項目を漏れなく紐付け

- 資産ごとに判定した具体的な弱点を記載し、それに対応するStep2・3の具体的な対策項目（権限強化やOS更新等）を漏れなく紐付けます。

実行マッピングテーブルの例

No.	資産名称 (P.30/32)	リスクレベル	弱点（脆弱性）の具体的な内容	対応すべき対策項目	実行責任者	完了期限（目標）
A-1	顧客マスターリスト (データ)	A (最優先)	共有フォルダが「Everyone」アクセス可能になっている。（P.50参照）	アクセス権限強化		
A-2	営業部 PC-005 (機器)	A (最優先)	1. OSバージョンが古い（例：Windows 10 21H2） 2. 対策ソフトが期限切れ。（P.54~55参照）	1. ソフトウェア更新（P.51~53参照※） 2. 対策ソフトの更新（P.54~58参照※）		
A-3	経理会計データ (データ)	A (最優先)	経理DBのバックアップデータがネットワークに接続されたままになっている。（P.70~72参照）	バックアップの隔離（P.70~72参照※）		
A-4	予備機 PC-012 (機器)	A (最優先)	OSがサポート切れ (Windows 7)。	機器の入れ替え または ネットワークからの即時切断		

※本例の対策についての内容を説明しているページ

マッピング手順

2. 「データ資産棚卸ワークシート」および「機器資産棚卸ワークシート」から、対策がとれていないチェック観点を抽出し、各観点に紐づく**Step2/3の対策項目**（例：アクセス権限強化、OSアップデートなど）を選択する。

マッピングテーブルの活用方法

1. 「弱点（脆弱性）の具体的な内容」には、「棚卸ワークシート」のマトリクスに記載している判定理由を用いて、パスワードが不十分、アクセス権が緩いなど、**具体的な問題点**を記載します。

Copyright© Japan Automobile Manufacturers Association, Inc.

対策項目のマッピングと担当者③

各対策に実行責任者と完了期限を割り当て　確実な実行に向けた計画の確定

- 各対策に対し、実行責任者と完了期限を明確に割り当て、いつまでに誰が何を完了させるかという具体的な活動計画を確定させてください。

実行マッピングテーブルの例

No.	資産名称 (P.30/32)	リスクレベル	弱点（脆弱性）の具体的な内容	対応すべき対策項目	実行責任者	完了期限（目標）
A-1	顧客マスターリスト (データ)	A (最優先)	共有フォルダが「Everyone」アクセス可能になっている。（P.50参照）	アクセス権限強化	情報システム部 / 佐藤	○月○日
A-2	営業部 PC-005 (機器)	A (最優先)	1. OSバージョンが古い（例：Windows 10 21H2） 2. 対策ソフトが期限切れ。（P.54~55参照）	1. ソフトウェア更新（P.51~53参照※） 2. 対策ソフトの更新（P.54~58参照※）	総務部 / 田中	○月○日
A-3	経理会計データ (データ)	A (最優先)	経理DBのバックアップデータがネットワークに接続されたままになっている。（P.70~72参照）	バックアップの隔離（P.70~72参照※）	情報システム部 / 佐藤	
A-4	予備機 PC-012 (機器)	A (最優先)	OSがサポート切れ (Windows 7)。	機器の入れ替え または ネットワークからの即時切断	総務部 / 田中	○月○日

※本例の対策についての内容を説明しているページ

マッピング手順

3. 対策の**実行責任者**（情報システム担当、総務担当など）をリストに明確に記入する。

実行責任者の定義

実行責任者は、対策の計画と進捗管理を行います。役割が曖昧だと対策が進まないため、総務部門が実行責任者となり、各部門の担当者に対策実行の協力を依頼します。

このマッピングにより、Step2以降の活動計画が具体的に確定します。

Copyright© Japan Automobile Manufacturers Association, Inc.

Step1の完了と次のアクション

対策の土台が完成　最大の山場を越え、実務的な防御に移る

- これで、「何を、なぜ守るのか」が明確になりました。
  このリストを基に、すぐに次のStep2（基本的な「入口」を確実に固める）へ移行します。

Step1.
守るべき「資産」を見える化する

情報資産の分類 → 資産リストの作成 → 対策の優先度 → 対策項目のマッピング

機密区分テーブル → 資産リスト / 機器資産リスト → リスクレベル決定マトリックス → マッピングテーブル

Step1完了チェックリスト

- ✅ 情報資産リスト（データ・機器）が完成した。
- ✅ リスク評価と優先度【A】が決定された。
- ✅ 対策項目のマッピングと担当者が決定した。
- ✅ 経営層に棚卸の結果を報告した。

Step1 完了

Step2.
基本的な「入口」を確実に固める

マッピングテーブル

次のアクション

- パスワードの強化
- 共通設定の見直し
- 4つの基本対策
- 防御の強化
- ウイルス対策

半期ごとに見直す
⇒Step0「情報収集」へ

次のステップは「実行」です。リストの優先度に基づき、すぐにアクションを開始しましょう。

Copyright© Japan Automobile Manufacturers Association, Inc.

4．Step 2 基本的な「入口」を確実に固める

【この章の内容】

・Step2の目的と全体像	：外部からの不正アクセスを防ぐための4つの基本対策を紹介
・パスワードルール：なぜ強化が必要か	：脆弱なパスワードが招くリスクと、ルールの具体例を説明
・パスワード管理の運用チェックリスト	：従業員への周知状況と、定期的な更新ルールの確認項目
・アクセス権限：制限の原則	：「必要な人だけ」がアクセスできる設定の基本と確認方法
・共有フォルダの権限設定手順	：共有設定の確認と、不要なアクセス権限を解除する手順を解説
・ソフトウェア最新化：緊急性	：OSやアプリの未更新がセキュリティホールになる理由を解説
・アップデートの運用手順チェック	：定期的な更新チェックと、適用を確実にするための手順
・ウイルス対策ソフト：導入の基本	：ウイルス対策ソフトの選定基準と、全端末への導入手順
・導入後の運用とパターンファイル	：定義ファイルの自動更新設定と、動作確認の手順を解説
・【コラム】クラウド利用の注意点	：データをクラウドに置く際の最低限のセキュリティ設定
・Step2完了のためのアクション	：4つの対策の実施状況を振り返る最終チェックリスト
・Step2全体の進捗確認	：Step2全体を完了するための アクションプランの確認

Copyright© Japan Automobile Manufacturers Association, Inc.

Step2の目的と全体像

最大の侵入経路を封鎖する　４つの基本対策で防御レベルを引き上げる

- Step1で特定した高リスク資産を守るため、外部からの侵入経路として最も狙われやすい箇所に対し、基本的な４つの対策を実行します。専門的な設定よりも、全員でのルール徹底が重要です。

4つの基本対策

パスワードの強化
パスワードルールの徹底

共通設定の見直し
アクセス権限の整理

ソフトの最新化
OSやアプリケーションの最新化

ウイルス対策
全端末への対策ソフト導入と運用

全従業員が対象です。
特にパスワード管理やソフトウェア最新化は個人の意識に依存します。
総務部門は、これらのルールが部門・個人レベルで確実に守られているかをチェックする役割を担います。

この4つの対策を確実に実施することで、最も頻繁な攻撃の約8割を防御することが可能と言われています。

Copyright© Japan Automobile Manufacturers Association, Inc.

パスワード強化が必要な理由

不正アクセスは「推測されるパスワード」から始まる　すぐに変更してください

- 攻撃者は自動ツールを使い、単純なパスワードを総当たりで試行します。簡単なパスワードや使いまわしは、鍵のない玄関と同じです。

推奨されるパスワードルール

1. **8桁以上**とする。(より安全には12桁以上を推奨)
2. **英大文字、英小文字、数字、記号**のうち**3種類以上を組み合わせる。**
3. サービスごとに**異なるパスワードを設定する**（使いまわし禁止）。
4. **パスワード管理ツール**（会社推奨のもの）の使用を推奨する。

1 桁パスワードの組合せ全通り ⇒ $(10 + 26 + 26 + 33 = 95$(通り)$)$
数字　英大　小文字　記号

1桁増えるごとに “×95” されていく（95×95×…）

⚠ 危険なパスワード例

(1)IDと同じ文字列	takahiro22
(2)自分や家族の名前、電話番号、生年月日	yamada, 090111222, 19960628
(3)辞書に載っている一般的な英単語	Password, baseball, soccer
(4)同じ文字列、わかりやすい並びの文字列	aaaa, abcd,qwerty

efUieU0HqcO+
e948&Uu/AMxE
6_Xl#c(y9aJt

全従業員に対し、このルールを即座に周知徹底し、パスワードの変更を指示してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

パスワードの使いまわしを回避する方法

パスワードの使いまわしは鍵のない玄関と同じ　個別のサービスごとに違うパスワードを設定しましょう

- パスワードの使いまわしが発生してしまうのは、パスワードを考えるのが面倒、覚えられない、などの理由が考えられます。ここで紹介するのは、サービスごとに作ることができ、覚えやすいパスワードのつくり方です。

参考：IPA, https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

1. コアパスワードをつくる

適当なコアフレーズを考える
→ 例：テレビが大好き

ローマ字変換
→ 例：terebigadaisuki

何通りかの変換をする（3通りあると安心）
→ 変換の例：大文字に変換／末尾に数字を追加／末尾に記号を追加

コアパスワード完成
→ 例：terebiGAdaisuki06&&

2. サービス毎の識別子を決める

	サービスごとの識別子		コアパスワード
サービス「**abc**クラウド」	**abc**	＋	terebiGAdaisuki06&&
サービス「**いろは**銀行」	**irh**	＋	terebiGAdaisuki06&&
サービス「**IPA**メール」	**IPA**	＋	terebiGAdaisuki06&&

サービスごとの識別子とコアパスワードを組み合わせることで**記憶可能なサイトごとのパスワード**を生成できる

このやり方を参考に、使いまわさなくて済むセキュアなパスワードを設定しましょう。

Copyright© Japan Automobile Manufacturers Association, Inc.

パスワード管理の運用チェックリスト

ルールだけでなく「運用」を徹底する　特に人事異動・退職時の対応が最重要

- パスワードのルールが定着しているか、また、退職者による不正アクセスリスクを防ぐための運用フローが確立されているかを確認します。

パスワード管理の運用チェックリストの例

No.	確認項目	確認の観点（チェックの視点）	担当者	状況	備考/課題
1	ルール周知の徹底 B社事例	新しいパスワードルール（P.43）を全従業員が理解し、誓約書や理解度テストなどを実施したか？	総務部	□ 完了	○○部で○○%の人がテスト未実施
2	新規採用/異動時の対応	新規アカウント発行時に、必ず強力な初回パスワードを設定し、ルールに基づき即時変更させているか？	情シス担当	□ 完了	初回パスワードの設定基準を文書化
3	退職時のアカウント処理	退職・休職・異動などでアクセス権が不要になったアカウントを、最終出社日までにすべて抹消またはロックしているか？	総務部	□ 完了	抹消フローをマニュアル化
4	パスワード管理方法	従業員がパスワードを紙の付箋やメモに残したり、共有ファイルに保存したりしていないかを、定期的に巡回チェックしているか？	総務部	□ 部分的	巡回チェックの頻度が不足
5	管理者アカウントの管理	サーバー、ルーター、重要なシステムなどの管理者アカウントのパスワードを、四半期に一度など定期的に変更しているか？	情シス担当	□ 完了	-
6	システム設定の強制	利用システム側で、パスワードの桁数、文字種などの強制設定が有効になっているか？	情シス担当	□ 完了	一部旧システムは手動対応が必要

運用フローの確認ポイント

1. 新しいパスワードルールが全従業員に周知され、理解度テストを実施したか？
2. 新入社員/異動者のシステムアカウントが即座に登録/変更されるフローが確立されているか？
3. 退職者のシステムアカウントが即座に抹消されるフローが確立されているか？
4. 紙や付箋にパスワードをメモしていないかを定期的に確認しているか？
5. 管理者アカウント（サーバー、ルーターなど）のパスワードが定期的に変更されているか？（パスワードが漏洩することを前提に考える場合 定期的な変更が必要）
6. システム側でパスワードの強制設定が有効になっているか？

このチェックリストに基づき、運用上の穴がないか、総務部門が確認と是正を四半期ごとに行ってください。

Copyright© Japan Automobile Manufacturers Association, Inc.

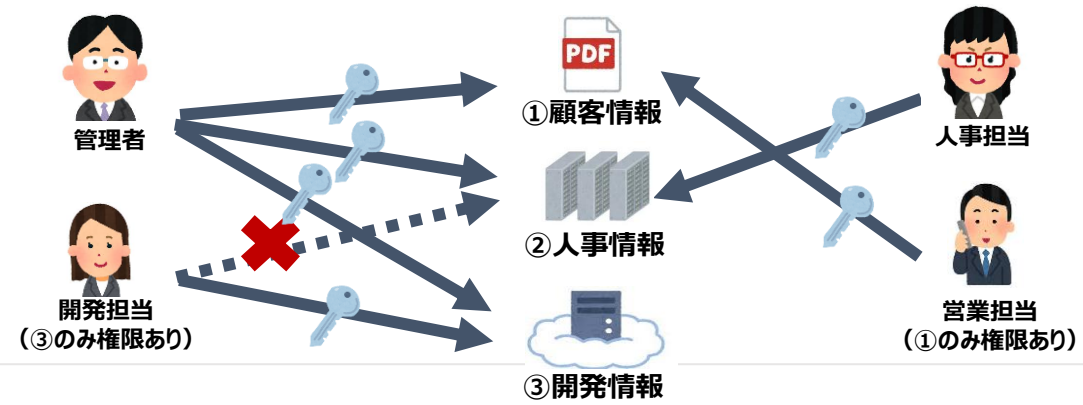
アクセス権限：制限の原則①

情報漏洩を防ぐ鉄則　必要な人だけに権限を絞る「最小権限」の導入

- 内部からの不正持ち出しや誤操作を防ぐため、全従業員に対し、業務遂行に必要な最小限のアクセス権限のみを与える運用を徹底します。

【最小権限の原則】

従業員には、業務遂行に必要な**最小限のアクセス権限**（読み取り、書き込み、削除など）のみを与えること。すべての人に「フルアクセス」を与える設定は、内部リスクを極大化させます。



最小権限の原則とは、
情報セキュリティや計算機科学などの分野において、コンピューティング環境の特定の抽象化レイヤー内での全てのモジュール（プロセス、ユーザー、プログラム）がその**正当な目的に必要とされる情報と計算資源のみにアクセスできるように制限する**設計原則である

Copyright© Japan Automobile Manufacturers Association, Inc.

アクセス権限：制限の原則②

重要資産の保管場所を特定　権限設定の妥当性を速やかに点検

- 重要度「高」のデータが保存されている場所の権限を最優先で確認し、最小権限の原則に基づいた具体的な設定変更を検討してください。

【権限設定の確認対象】

最小権限の原則に基づいた権限設定を検討するために、
高リスク資産の権限（誰にどんな権限を与えるのか）を整理してください。
特に、重要度「高」のデータが保存されている場所の権限を最優先で確認してください。（P.30~33のリスト参照）

※確認対象の例

- **共有フォルダ（ファイルサーバー）**
- **顧客管理システムや会計システム**
- **グループウェアやクラウドストレージ**

P.37~39のマッピングリストに基づき、高リスク資産の権限はすぐに整理してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

アクセス権限の適切な管理①

発行・変更は承認制　異動・退職時に即座に削除できる管理ルールの策定

- 情報漏洩や不正アクセスを防ぐ上で、アクセス権限の適切な管理は最も基本的な防御策です。特に、必要以上の権限を付与しない**「最小権限の原則」**を徹底し、社内外のシステムや情報資産へのアクセス状況を定期的に見直すことが重要です。

アクセス権限管理のルール化と実践

ルール策定:

あらゆるシステム・情報資産（共有フォルダ、社内システム、クラウドサービス、外部情報システム）へのアクセス権限について、以下のルールを定めます。

- **発行・変更・削除は申請・承認制**とし、権限の範囲は業務に必要な最小限に限定する。
- 人事異動や退職時には、速やかにアクセス権を削除・変更するフローを確立する。
- **外部情報システムの利用時も同様のルール**を適用し、守秘義務契約の締結や利用サービスの一覧化を行う。

ルール実践:

定められたルールが、全てのアクセス権限の管理において確実に実行されていることを確認します。

Copyright© Japan Automobile Manufacturers Association, Inc.

アクセス権限の適切な管理②

共有フォルダ等の全権限を棚卸　「Everyone」等の広範な設定を即座に是正

アクセス権限の定期的な棚卸

棚卸実施:

定期的に（例：四半期に一度）、全てのシステムや共有フォルダ、利用中の外部情報システムにおけるアクセス権限設定を棚卸します。

- **特に注意：**「Everyone」や「Guest」といった広範なアクセス権限が意図せず付与されていないかを確認し、速やかに解除・変更
- 不要なアカウントや退職者・異動者のアクセス権が残存していないかを確認し、削除

管理責任者の任命:

各システムや共有フォルダ、外部情報システムごとに管理責任者を任命し、棚卸と設定見直しを義務付けます。

【実践のポイント】

- **Step1で特定した「リスクA」の情報資産**を中心に、早急にアクセス権限の見直しを行います。
- ルールや運用フローは**「アクセス権限チェックリスト」**として文書化し、総務部門などが定期的に監査・是正を行います。

Copyright© Japan Automobile Manufacturers Association, Inc.

アクセス権限の適切な管理③

チェックリストによる定期監査　不備に対する迅速な改善・修正サイクルの確立

- Step1で特定した「リスクA」の情報資産を中心に、早急にアクセス権限の見直しを行います。

アクセス権限チェックリストの例

No	確認項目	確認の観点（チェックの視点）	担当者	状況	備考/課題
1	アクセス権限の管理ルール	アクセス権限の発行・変更・削除に関する**申請・承認ルール**が明文化され、全従業員に周知されているか。	総務部/情シス	□ 完了	-
		業務に必要な最小限の権限のみ付与する**「最小権限の原則」**がルールに明記されているか。	総務部/情シス	□ 完了	-
		人事異動・退職時のアカウント削除・変更フローが明確で、担当者に周知されているか。	総務部/情シス	□ 完了	-
2	共有フォルダ・社内システムのアクセス権	共有フォルダや社内システムで、「Everyone」や「Guest」権限が付与されていないか。	各部署管理者	□ 確認中	一部古い共有フォルダにEveryone 権限が残存
		各情報資産（Step1で特定）に対し、**業務上必要な部署・担当者のみに限定したアクセス権**が設定されているか。	総務部/情シス	□ 部分的	開発部共有フォルダに営業部員がアクセス可能
		退職・異動者のアカウントやアクセス権が、最終出社日までに全て削除・変更されているか。	総務部/情シス	□ 完了	-
3	クラウドサービス・外部情報システムのアクセス権	利用中のクラウドサービス・外部情報システムが**全て一覧化**され、利用ルールに基づき承認されているか。	総務部/情シス	□ 完了	-
		各サービスの**共有設定やアクセス権限が適切に設定**され、意図しない全体公開等がないか。	各部署管理者	□ 確認中	OneDrive で一部ファイルが外部公開設定
		利用終了済みの外部サービスアカウントが残存していないか、または権限が解除されているか	総務部/情シス	□ 部分的	過去プロジェクトのクラウドサービスアカウントが未削除
4	定期的な棚卸と見直し	全てのアクセス権限について、**定期的な棚卸**が実施され、その記録が保管されているか。	総務部/情シス	□ 部分的	四半期ごと実施だが、クラウドサービスは年一回
		棚卸の結果、不要なアクセス権やアカウントが速やかに削除・是正されているか	総務部/情シス	□ 完了	-

Copyright© Japan Automobile Manufacturers Association, Inc.

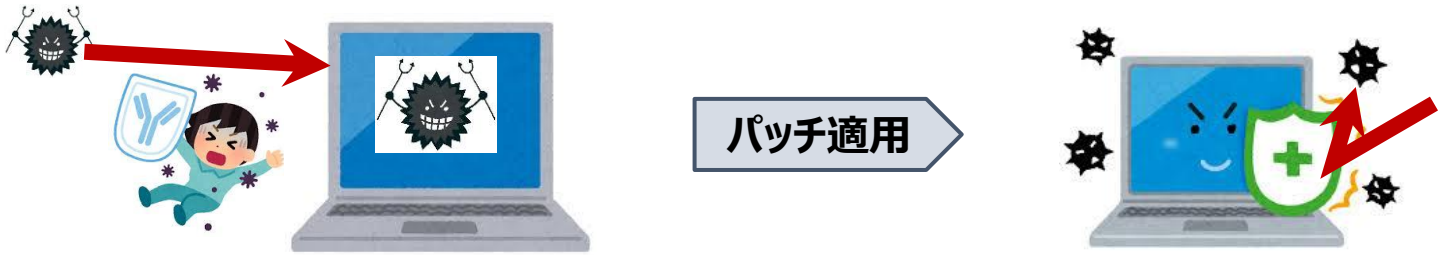
ソフトウェア最新化：緊急性①

脆弱性放置のリスクを理解　速やかなシステム最新化を徹底

- ソフトウェアの「脆弱性」は公開と同時に攻撃の標的となります。放置が致命的な侵入口となるリスクを再認識し、速やかな最新化を徹底してください。

【脆弱性放置のリスク】

脆弱性が発見されると、その情報はインターネット上に公開されます。
ソフトウェア最新化を遅らせることは、攻撃者に対し「ここに穴がある」と教えているのと同じです。
マルウェア感染やデータ漏洩のリスクが急激に高まります。⇒ 緊急に最新化が必要



Copyright© Japan Automobile Manufacturers Association, Inc.

ソフトウェア最新化：緊急性②

パッチ適用による弱点の克服　優先対象端末の即時更新

- Windows Update等のパッチ適用をルール化し、特にサポート切れOSは即座に利用停止、または最新機器への入れ替えを断行してください。

【緊急にソフトウェア最新化が必要な対象】

- OS全般（Windows, Mac, Linuxなど）
- Webブラウザ（Chrome, Edgeなど）
- 業務上重要なアプリ（Office製品、PDFリーダー、Java、Flash（使用している場合）など）
- システム基盤（VPN、ネットワーク機器、ファームウェア、ミドルウェア、など）

※特にP.53で特定した**サポート切れOS**は、**即座に利用停止**または**入れ替え**が必要です。

ソフトウェア最新化の方法（例）

・Windowsなどは、**Windows Update**を行う

・その他のアプリは各アプリの提供元の**情報を定期的に確認**（「更新オプション」＞「今すぐ更新」など）

P.24~25「脅威情報の収集」で確認した結果から最新化を行う

ソフトウェア最新化を「後回し」にすることは、侵入リスクを意図的に高めているのと同じです。

Copyright© Japan Automobile Manufacturers Association, Inc.

アップデートの運用手順チェック

従業員任せにしない「自動更新」の仕組みを整備する

- 個人の意識に頼るのではなく、強制力のある自動更新の運用が不可欠です。
  システム管理者（情報システム担当など）が主導し、以下の手順をチェックしてください。

アップデートの運用手順チェックリストの例

No.	確認項目	確認の観点（チェックの視点）	担当者	状況	備考/課題
1	OSの自動更新設定	Windows/MacなどのOSについて、全PCで自動更新機能が有効になっているか？	情シス担当	□ 完了	サーバーは手動運用（No.4で管理）
2	更新時間帯の設定	業務に支障が出ないよう、更新や再起動が業務時間外（例：深夜、週末など）にスケジュールされているか？	情シス担当	□ 完了	-
3	アップデートのログ確認	自動更新の適用が失敗していないかを、システムログや管理ツールで定期的に（例：月次）確認しているか？	情シス担当	□ 部分的	確認ツール導入の予算が未確保
4	サーバー/共用PCの管理	サーバーや共用PCなど、特定端末の手動更新を責任持って行う担当者が明確になっているか？	情シス担当	□ 完了	担当者リストを作成し、周知
5	サポート切れOSの特定	P.32の機器リストに基づき、サポート切れのOS（例：Windows 7、古いOSバージョンのAndroid）を搭載した機器が残存していないか？	総務部	□ 完了	該当機器（PC-012）はネットワークから隔離済み
6	業務アプリの更新管理	Adobe Reader、Webブラウザなど、業務上利用頻度の高いアプリケーションについても、自動更新設定が有効になっているか？	情シス担当	□ 部分的	一部インストールソフトは手動更新が必要

アップデートの運用手順の確認ポイント

1. OSの自動更新機能が有効になっているか？
2. 業務に支障がない時間帯（深夜など）に更新が行われる設定か？
3. 自動更新が失敗していないかを示すログを定期的に確認しているか？
4. サーバーや共用PCなど、特定端末の更新が滞っていないかを確認する担当者が割り当てられているか？
5. サポート切れの古いバージョンを使用している端末がないか？（P.32と再照合）
6. 利用頻度が高いアプリケーションの自動更新設定が有効になっているか？

更新プログラムの適用遅れは、即座にStep1の「リスクA」に該当することを全従業員に周知徹底してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

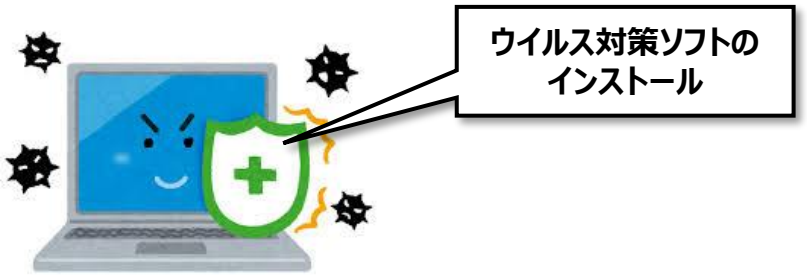
ウイルス対策ソフト：導入の基本①

侵入を防ぐ最後の砦　全部門・全端末へのソフト導入を確認

- マルウェア侵入を水際で防ぐため、全PC・サーバーに会社推奨ソフトが導入されているか、期限切れがないか点検し、未導入端末を即座に解消します。

【導入状況の確認】

P.32~33の機器リストに基づき、**全PC、サーバー、業務用スマートフォン**に、会社が推奨する
ウイルス対策ソフトがインストールされているかを確認します。
未導入・期限切れとなっている端末は即座に是正します。
※オフライン端末でもUSBメモリなどからウイルス感染の事例有り



Copyright© Japan Automobile Manufacturers Association, Inc.

ウイルス対策ソフト：導入の基本②

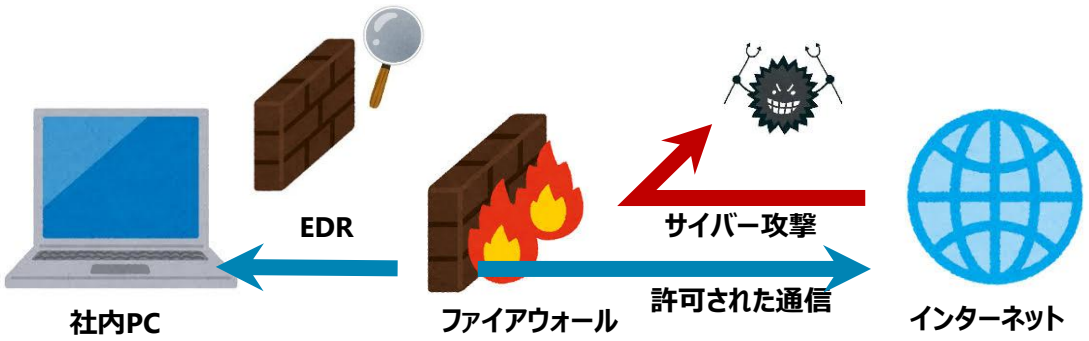
未導入・期限切れの即時解消　最新脅威に対応した製品の選定

- ランサムウェア等の最新脅威に対応するため、不審な挙動を検知・ブロックできるEDR機能等を備えた最新ソフトを選定し、導入を完了させてください。

【製品の機能確認】

現代の脅威（ランサムウェアなど）に対応するため、単なるウイルス検知だけでなく、 A社事例 D社事例

不審な挙動を検知・ブロックする機能（EDRなど）を持つ最新のソフトを選定し、導入してください。



未導入・期限切れの端末は、最も侵入リスクが高い状態です。直ちに是正してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

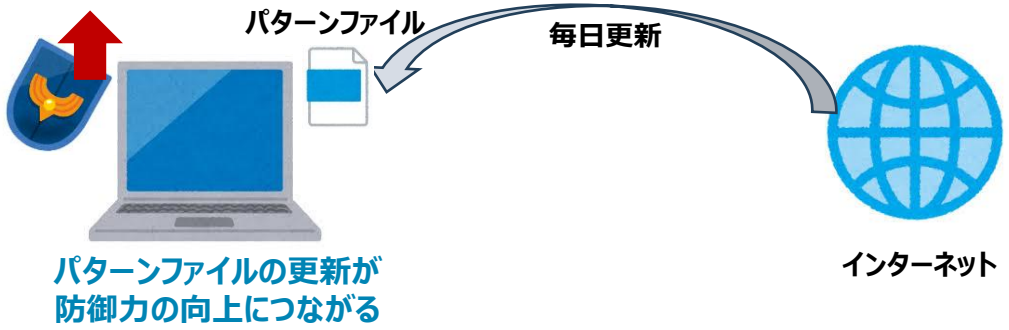
導入後の運用とパターンファイル①

継続的な運用が生命線　定義ファイルの「自動更新」を徹底

- 対策ソフトは、最新の「脅威リスト（パターンファイル）」を常に更新しなければ効果を発揮しません。ソフトが正しく機能しているかの運用管理が重要です。

【パターンファイルの自動更新】

パターンファイルは、新しいウイルスに対応するための「定義ファイル」です。
これが古いままだと、最新の攻撃に対応できません。
必ず**自動更新設定が有効になっているか**、**パターンファイルの更新が行われているか**
確認してください。



Copyright© Japan Automobile Manufacturers Association, Inc.

導入後の運用とパターンファイル②

自動スキャンの実行と異常検知　管理者への即時報告体制の構築

- クイックスキャンやフルスキャンの自動実行の確認、問題発生時の迅速な対応のための報告フローの確立が重要となります。

【スキャンと管理】

スキャン
毎日の起動時にクイックスキャン、
週末などにフルスキャンが**自動実行されているか**を確認

管理
ソフトが警告を発した際の
報告フロー（P.65へ接続）を確立し、
担当者が迅速に対応できるようにする

警告やエラーを無視せず、担当者が必ずログをチェックし、問題があれば P.65のフローで報告する体制を確立してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

ウイルス対策ソフトの運用手順チェック

個人の意識に頼るのではなく、情シスが主導し運用状況を定期的に確認

- ウイルス対策ソフトは「導入して終わり」ではありません。最新の脅威に対応し、常に効果を発揮させるためには、適切な運用管理が不可欠です。

アップデートの運用手順チェックリストの例

No.	確認項目	確認の観点（チェックの視点）	担当者	状況	備考/課題
1	パターンファイルの自動更新状況	全てのPC・サーバーでパターンファイルの自動更新設定が有効になっているか？（P.32,57参照）	情シス担当	□ 完了	
2	パターンファイルの最新性確認	パターンファイルが常に最新の状態に維持されているか？	情シス担当	□ 完了	-
3	定期スキャン実施状況	定期的なフルスキャン/クイックスキャンが自動で実施され、完了しているか？（P.32,57参照）	情シス担当	□ 部分的	一部PCでスキャンが手動設定
4	全端末への導入状況	Step1の機器リスト（P.32~33参照）に基づき、全てのPC・サーバーにウイルス対策ソフトが導入されているか？	総務部	□ 完了	
5	警告・エラー時の報告・対応フロー	ウイルス対策ソフトの警告やエラー発生時の報告フローが確立され、迅速に対応できるか？（P.57参照）	情シス担当	□ 部分的	担当者への通知遅延の可能性
6	ライセンス・契約の確認	ウイルス対策ソフトのライセンス期限が切れていないか？定期的に契約内容を見直しているか？	総務部	□ 完了	

ウイルスソフト対策は、導入後の「継続的な運用管理」が生命線です。
このチェックリストを活用し、定期的な見直しを習慣化してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

【コラム】クラウド利用の注意点①

クラウドは便利だが、設定ミスが「情報漏えい」に直結する

- クラウドサービスの利用は便利ですが、アクセス権限や共有設定のミスが、インターネット全体への情報公開に繋がる最大の要因です。ここでは事例を紹介します。

【共有設定の原則】

事例① クラウドサービスの設定ミスによる情報漏洩

「クラウドストレージのアクセス権限設定不備により、機密情報が外部に公開・流出」

原因：「クラウドの設定ミス」

自動車部品メーカーが利用していたクラウドストレージの**アクセス権限設定を誤り**、**社外から誰でも閲覧可能な**状態になっていた。

クラウドベースのプロジェクト管理ツールで、社外共有機能の設定を誤り、**開発中の新製品情報が公開状態**になっていた。

対策：「共有設定の見直し」

アクセス権限や共有範囲を最小限に設定。
月に一度など**定期的に設定内容を監査**し、不備がないか確認する。

特に初期設定や新機能導入時に見落としが発生しがちです。
アクセス権限や公開範囲の設定は、情報漏洩に直結するため、**定期的な見直しと厳格な管理が不可欠**です。

Copyright© Japan Automobile Manufacturers Association, Inc.

【コラム】クラウド利用の注意点②

クラウドは便利だが、認証情報の管理ミスが「不正アクセス」に直結する

【アカウントの強化】

事例② クラウド環境への不正アクセスによるデータ改ざん・破壊

「不正アクセスで設計データが改ざん、またはランサムウェア感染で生産管理システムが停止」

原因：「認証情報の管理不備」

自動車メーカーのサプライヤーが利用していた**クラウド上の開発環境に不正アクセスされ、設計データが改ざん**された。

クラウド上のデータベースがランサムウェアに感染し、生産管理システムが停止。復旧に時間を要し、生産ラインにも影響が出た。

対策：「アカウントの強化」

- ■「パスワードの強化」
- ■「ウイルス対策ソフトの導入」
- ■「ネットワーク外でのバックアップやデータ保管」

推測困難なパスワード設定と**多要素認証を徹底**。
ウイルス対策ソフトの導入に加え、**オフラインバックアップ**と、システム停止時の**代替生産計画を準備**する。

クラウド利用状況は P.32~33 の機器リストに追加し、設定を定期的にチェックしてください。

Copyright© Japan Automobile Manufacturers Association, Inc.

Step 2完了のためのアクション

基本の「入口対策」完了　ウイルス対策の運用チェックリストのチェック項目に「✓」が入ったか

- 4つの基本対策の完了をもって、貴社のセキュリティ体制は大きな一歩を踏み出しました。残る「未実施」項目がないか、必ずダブルチェックを行い、次のステップへ進む準備をしてください。

Step 2
基本的な「入口」を確実に固める

パスワードの強化 | **共通設定の見直し** | **防御の強化** | **ウイルス対策**

パスワード運用

共有フォルダ

アップデート

ウイルス対策運用

Step 2 完了

マッピングテーブル

パスワード運用
共有フォルダ
アップデート
ウイルス対策運用

Step1・2でPDCA回す

定期的な棚卸(最新化)

ステップ３へ進む

もしもの事態に備える

Step2完了チェックリスト

- ✅ 新しいパスワードルールが徹底され、退職者・異動者のアカウント処理が完了した。
- ✅ P.39のリストに基づき、高リスク資産のアクセス権限の整理が完了した。
- ✅ OS/ソフトウェアの自動更新体制が整備された。
- ✅ ウイルス対策ソフトの導入と運用（パターンファイル更新）が定着した。

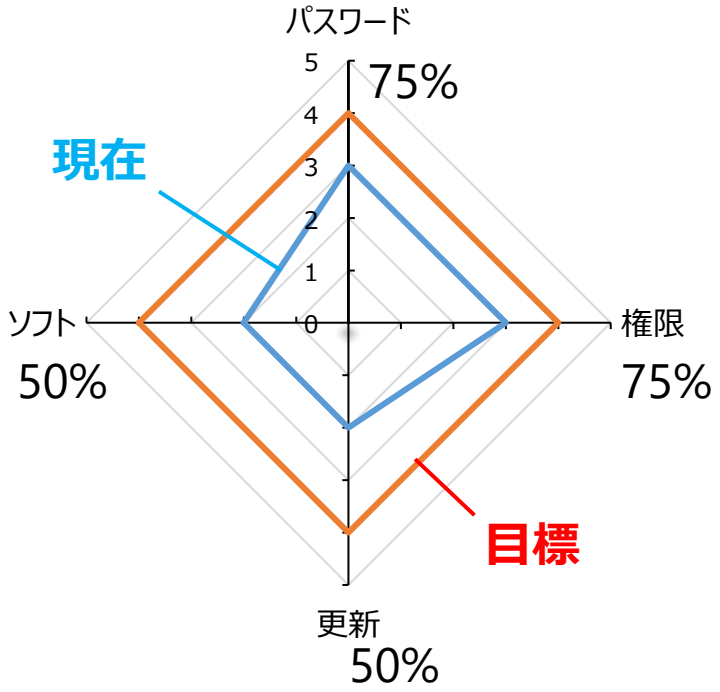
もし未完了の項目があれば、P.39のマッピングリストに戻り、担当者と期限を再設定してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

Step 2全体の進捗確認

対策は継続中　経営層への報告（P.15~17）のため、目標達成度を評価する

- これまでの活動の目標達成度を評価します。この評価結果は、P.15~17の経営層への報告の基礎資料となります。客観的な評価を行い、次期計画へと繋げます。



評価の手順

1. 対策軸ごとの達成度評価： P.45,50,53,58のチェックリストに基づき、パスワード、アクセス権限、更新管理、ウイルス対策の4軸で達成度をパーセントで評価します。
2. 未達成項目と課題：なぜ未達成なのか（予算不足、工数不足など）を特定し、次期アクションプランを策定します。

この評価をもって、継続的な支援を得るための報告準備に入ります。

Copyright© Japan Automobile Manufacturers Association, Inc.

5．Step 3「もしも」の事態に備える

【この章の内容】

・Step3の目的と全体像	：インシデント発生時の被害を最小限に抑える準備を紹介
・緊急連絡体制：初動フロー図	：攻撃発生時に誰に何を報告するかを明確にするフロー図
・連絡先のリスト化と訓練計画	：社内・社外の緊急連絡先をまとめるためのテンプレート
・データバックアップ：手順と重要性	：なぜネットワーク外にデータを保存すべきか、手順を解説
・バックアップ運用チェックリスト	：定期的な実施状況と、データ復元テストの確認項目
・生産継続：サーバーダウンに備える	：サーバー停止時でも生産を止めないための代替手段の検討
・BCP（事業継続計画）の簡易作成	：業務を一時的に代替する際の最小限の計画作成シート
・Step3完了のためのアクション	：3つの対策の実施状況を振り返る最終チェックリスト

Copyright© Japan Automobile Manufacturers Association, Inc.

Step3の目的と全体像

防御が破られても、事業を止めない　被害を最小化する「備え」こそが信用を守る

- サイバー攻撃は100%防げません。万が一、ランサムウェア感染やシステム停止が発生した場合のパニックを抑え、迅速に対応するためのマニュアルを作成します。

3つの緊急対策

初動体制
異常発見時の連絡・報告フローの確立（パニック防止）

データ防衛
バックアップデータの隔離（復旧の生命線）

業務継続
システム停止時の代替業務の定義（事業停止回避）

マニュアルの重要性
危機発生時は冷静な判断が難しくなります。
作成したフロー図やリストは、システムが使えない状況を想定し、紙で印刷・保管することをお勧めします。

このStepの完了は、貴社の事業継続計画（BCP）の基礎を築くことを意味します。

Copyright© Japan Automobile Manufacturers Association, Inc.

緊急連絡体制：初動フロー図

異常を感知したら「即座に隔離、そして電話」 パニックを回避する5分ルール

- ランサムウェア感染やシステム異常を発見した従業員は、パニックに陥ることなく、このシンプルな手順に従って行動してください。最初の5分間の行動が被害の拡大を防ぐ鍵となります。

C社事例

【異常発見者：最初に行う「3つの緊急行動」】

異常を発見したら、すぐに以下の行動をとってください（**被害端末の電源は切らない！**）。

ネットワーク切断 → 画面の状態を記録 → 即座に電話

マルウェア拡散を防ぐ
自分のPCからLANケーブルをぬき、Wi-Fiをオフにする。マルウェアの水平感染（拡散）を物理的に防ぎます

証拠の保全
エラーメッセージ、身代金要求画面などをスマートフォンで撮影し、証拠を保全します。

管理者への報告
周囲の人に状況を説明する前に、管理者へP.66のリストを使って電話で報告します

【管理者（報告を受けた担当者）の行動】

管理者は報告を受けたら速やかに状況把握しエスカレーションしてください

情報収集 → 隔離の指示 → 上層部へ報告

状況の把握
被害状況（どのPCか、どのフォルダが暗号化されたか）を電話で聴取します

被害範囲の限定
被害端末だけでなく、周辺のPCに対しても一時的なネットワーク切断を指示し、被害範囲を限定します

エスカレーション
P.66の緊急連絡リストに基づき、部門長・経営層へ状況を報告し、外部ベンダーへの連絡（エスカレーション）の可否を仰ぎます

このフロー図を印刷し、全従業員がアクセスできる場所に必ず掲示してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

連絡先のリスト化と訓練計画①

パニック時でもすぐに参照できる、「システムが使えない前提」の連絡帳

- 事故発生時は、メールや社内チャットは利用できない前提で動く必要があります。紙で印刷・保管する緊急連絡先リストを作成し、訓練を通じてその有効性を検証します。 D社事例

【緊急連絡先リスト（紙で保管）の作成と保管場所】

以下の情報を記入したリストを、各部署のホワイトボード横や緊急時マニュアルファイルなどに印刷して保管してください。
社内対応チーム： 推進責任者、情報システム担当者、経営者（判断権者）の氏名、内線、個人の携帯電話番号（夜間・休日連絡用）
外部専門家　　： 契約中のセキュリティベンダーのサポートデスク、サーバー保守業者の24時間窓口電話番号と契約番号。

緊急連絡先リストの例

No.	役割	氏名 / 部門名	メールアドレス	電話番号	備考
1	推進責任者	○○ / 総務部	△△△@××××	[内線]000-0000-0000 [緊急用]000-0000-0000	9:00-17:00
2	情報システム担当者				9:00-17:00
3	経営者（判断権者）				9:00-17:00
4	外部専門家（サポートデスク）			[緊急用]000-0000-0000	24時間対応

このリストは、人事異動や契約ベンダーの変更があった際に、すぐに更新する体制を確立してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

連絡先のリスト化と訓練計画②

緊急連絡先リストが機能するのか、訓練計画を立案する

【初動対応訓練の具体的な実施内容】

訓練計画立案

リストが作成されたら、それが機能するかを確認するための訓練（訓練計画）を組みます。

■ 訓練内容：「経理部のPCが暗号化された」などのシナリオを設定し、発見者役、管理者役、経営者役に分かれて、P.65のフロー通りに電話連絡のみで報告と指示が行えるかを確認します。

■ 頻度　　：最低でも半期に一度実施。

訓練計画立案

訓練内容	頻度	役割	氏名/部門名	評価	課題	対策
「経理部のPCが暗号化された」	半期に一度	発見者役	△△ / 総務部			
		管理者役	・・・			
		経営者役	・・・			

訓練は、緊急連絡先リストが機能するのかを判断する重要な実践の場です。

Copyright© Japan Automobile Manufacturers Association, Inc.

連絡先のリスト化と訓練計画③

緊急連絡先リストが機能するのか、実践する

【初動対応訓練の具体的な実施内容】

訓練実施と訓練評価

訓練計画を立案したら、実施頻度に基づき訓練を実施し、評価を行います。

■　訓練実施と訓練評価：「報告は5分以内に行われたか？」「外部ベンダーへの連絡はスムーズだったか？」などを評価項目として設定し、計画に基づき訓練を実施します。

訓練計画立案 → **訓練実施と訓練評価**

訓練内容	頻度	役割	氏名/部門名	評価	課題	対策
「経理部のPCが暗号化された」	半期に一度	発見者役	△△ / 総務部	報告は5分以内に行われた		
		管理者役	・・・	外部ベンダーへの連絡はスムーズだった		
		経営者役	・・・			

訓練を実施・評価することで、意味のある訓練となります。

Copyright© Japan Automobile Manufacturers Association, Inc.

連絡先のリスト化と訓練計画④

緊急連絡先リストの機能性の向上のため、振り返る

【初動対応訓練の具体的な実施内容】

振り返り

訓練を実施・評価したら、リストの改善に向けた振り返りを行います。

■　振り返り：設定したそれぞれの評価項目に対して、訓練実施においてどのような課題があったのか、課題に対してどのような対策を打つのか、振り返りを実施します。

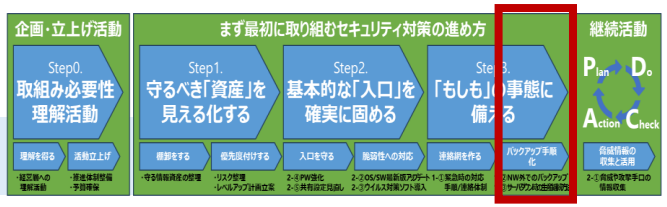
訓練計画立案 ＞ 訓練実施と訓練評価 ＞ **振り返り**

訓練内容	頻度	役割	氏名/部門名	評価	課題	対策
「経理部のPCが暗号化された」	半期に一度	発見者役	△△ / 総務部	報告は5分以内に行われた	連絡先リストや報告フローが見にくく、報告に手間取った	・連絡先リストや報告フローの見直し ・保管場所の周知
		管理者役	・・・	外部ベンダーへの連絡はスムーズだった	情報が更新されていなかった	・リストの見直し
		経営者役	・・・			

訓練の振り返りが、作成した緊急連絡先リストの有効性に直結します。

Copyright© Japan Automobile Manufacturers Association, Inc.

データバックアップ：手順と重要性①



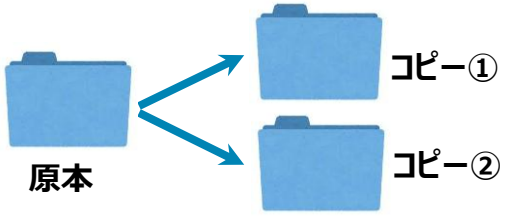
確実なデータ復旧のための鉄則 「3-2-1ルール」の全社的な徹底

- バックアップを原本含め3つ持ち、2種類以上のメディアに保存し、1つをネットワーク外に置く「3-2-1ルール」を、すべての重要資産に適用してください。

【バックアップの基本原則：3-2-1ルール】

- ■ **3つ**のコピー　　：データを3つ（原本＋2つのバックアップ）持つ。
- ■ **2種類**のメディア　　：データを2種類以上のメディア（例：サーバーHDDと外部HDD/クラウド）に保存する。
- ■ **1つを**遠隔地/オフライン：少なくとも1つを物理的または論理的にネットワークから隔離する。

データは３つ作成

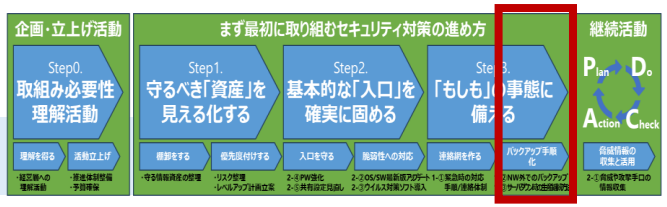


２種類のメディアに保存

１つは遠隔地に保存

Copyright© Japan Automobile Manufacturers Association, Inc.

データバックアップ：手順と重要性②



ランサムウェアの二次被害防止　ネットワークからの物理的な隔離の徹底

- 外部HDD等を使用する場合は、使用時以外は物理的に接続を外す「オフライン保管」を徹底し、バックアップデータの暗号化被害を防ぎます。

D社事例

【ランサムウェア対策：隔離の原則（オフライン化）】

ランサムウェアはネットワークを通じてバックアップデータも暗号化します。

外部HDDを使用する場合は、使用時以外はPCやサーバーから接続を切って**オフライン保管**することを徹底してください。クラウドサービスの場合は、アクセス権を厳しく制限してください。

P.29で重要度「高」としたデータは、必ず3-2-1ルールに基づきバックアップされていることを確認してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

バックアップ運用手順チェック

バックアップは「復元できること」がすべて　定期テストを怠らない

- バックアップデータが破損していては意味がありません。データが確実に復元できるかを検証し、物理的な保管場所が安全かを確認します。

バックアップ運用のフロー

バックアップ実行

隔離

テスト環境で復元

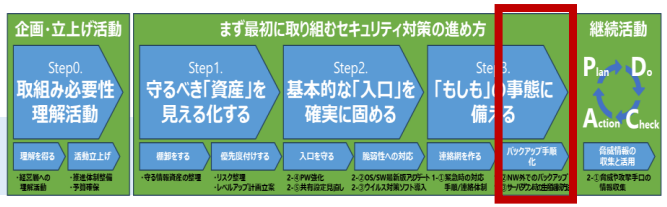
バックアップ運用チェックリストの例　D社事例

チェック項目	データ資産リストに基づく資産名 顧客マスターリスト(最新版)	R7年度 新規技術開発計画	社員人事評価データ	R6年度備品購入履歴	経理会計データ(過去3年)
バックアップがスケジュール通り自動実行されているか	○	○	○	×	○
バックアップデータがネットワークから完全に隔離されているか	・・・				
バックアップメディアが施錠された安全な場所に保管されているか	・・・				
復元テストを四半期に一度実施し、データを正しく戻せるか検証しているか	・・・				
バックアップからの復元手順書（マニュアル）が作成されているか	・・・				

復元テストの記録は、P.12の経営層への報告（対策達成度）に含めてください。

Copyright© Japan Automobile Manufacturers Association, Inc.

生産継続：サーバーダウンに備える①



システム停止時の被害を最小化　目標復旧時間と目標復旧時点を明確に定義

- 重要データを使用する業務ごとに、システム停止を許容できる限界時間（RTO）等の指標を定め、復旧の目処を立てる基準としてください。

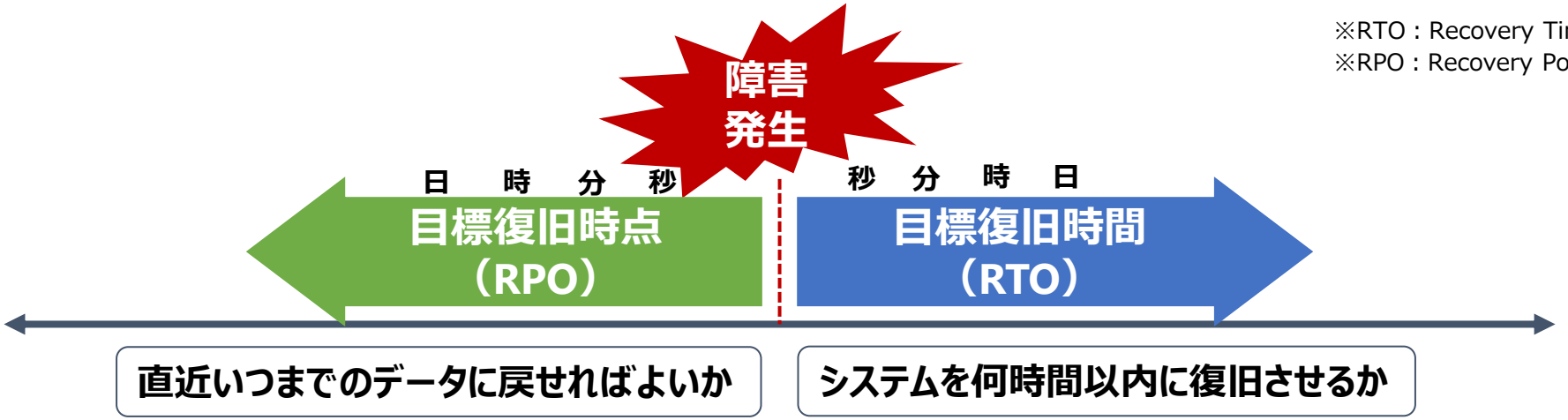
【目標復旧時間および目標復旧時点の定義】

P.30~33の資産リストに基づき、重要度「高」のデータを使用する業務について、以下の指標を定めます。

■ **目標復旧時間（RTO※）** ： システムを何時間以内に復旧させるか

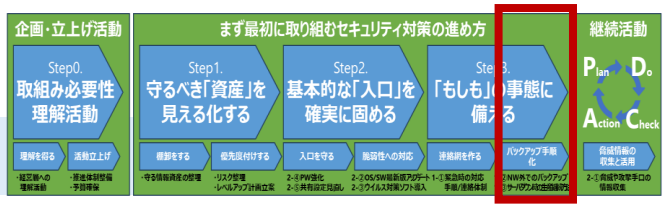
■ **目標復旧時点（RPO※）** ： 直近いつまでのデータに戻せればよいか（バックアップ頻度に影響）

※RTO：Recovery Time Objective
※RPO：Recovery Point Objective



Copyright© Japan Automobile Manufacturers Association, Inc.

生産継続：サーバーダウンに備える②



手作業や代替手段（紙・電話等）による、重要業務を止めない備え

- システム停止中も受注や出荷を止めないよう、手書き伝票やFAX、電話等を用いた代替運用の具体的な手順を準備しておきましょう。

A社事例

【代替業務の検討】

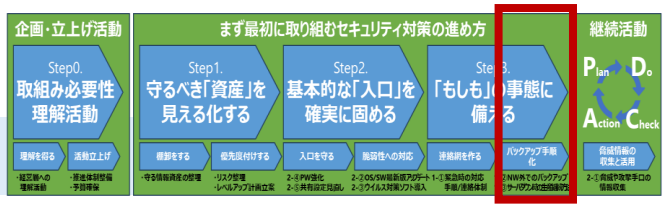
システムが使えない期間に、紙、電話、FAX、限定的なPC利用など、
手作業で**最低限の業務を行う方法**を検討します。

例：受注処理→紙伝票に記入し、システム復旧後にまとめて入力

特に「受注」「生産管理」「出荷」など、事業の根幹に関わる業務について代替手段を検討してください。

Copyright© Japan Automobile Manufacturers Association, Inc.

BCP（事業継続計画）の簡易作成①



「もしも」の時、事業を守る「最小限の羅針盤」を準備する

- サイバー攻撃によるシステム停止は、事業と信頼に甚大な影響を与えます。「簡易BCP」は、緊急時の行動を明確にし、早期復旧を促します。貴社独自のBCPを、今すぐ作成しましょう。

A社事例

【中小企業にこそ簡易BCPが不可欠な理由】

1. **複雑なBCPは不要**：
   リソースの限られた中小企業向けに、サイバー攻撃によるシステム停止という**喫緊のリスクに特化した「簡易版」**を作成します。
2. **事業停止の「空白期間」を埋める**：
   ランサムウェア感染などによるシステムダウンで業務が麻痺する際、事前の行動指針が**事業存続の命運**を分けます。
3. **信頼維持の基盤**：
   迅速な初動と事業再開能力は、**顧客・取引先からの信頼維持とサプライチェーン責任**を果たす上で不可欠です。

【テンプレートの目的と利用方法】

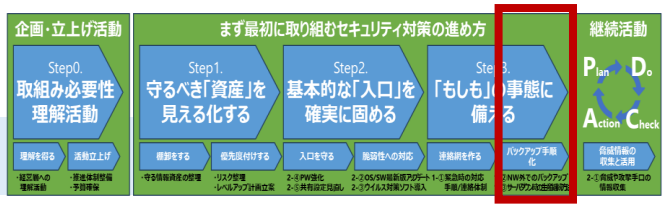
この簡易BCPは、「紙で印刷し、システムが使えない状況でも参照できる」ことを前提とします。以下の3ステップで、貴社の「羅針盤」を作成しましょう。

1. **要素の洗い出し**：危機発生時に**必要な情報（連絡先、重要業務、代替手段など）**をリストアップします。
   （これまでのStepを活用！P.30~33「**情報資産リスト**」、P.65「**初動フロー図**」、P.66~69「**緊急連絡先リスト**」、P.70~71「**バックアップ情報**」が参考になります。）
2. **テンプレートへの整理**：洗い出した要素を、次ページ「**BCP簡易表テンプレート**」に整理して記入します。
3. **訓練と見直し**：作成したBCPが機能するかを、**定期的な訓練**（P.66~69）で検証し、改善を継続します。

このシートの作成・印刷をもって、システムダウンへの備えが完了します。

Copyright© Japan Automobile Manufacturers Association, Inc.

BCP（事業継続計画）の簡易作成②



BCP簡易表テンプレート：緊急時に迷わない『行動指針』

- このBCP簡易表は、サイバー攻撃によるシステム停止時の行動指針です。
  Step0~3の情報から「誰が、何を、どうするのか」を具体化し、危機を乗り越えましょう。

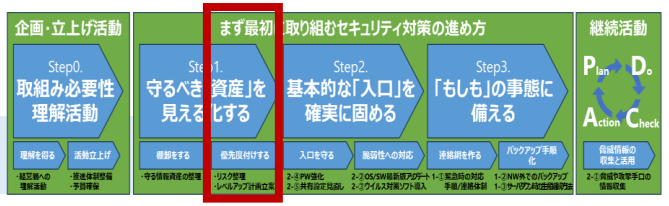
これまでの検討結果を集約した簡易版BCPの例

No.	項目名	目的	記載例	担当部門 / 責任者	参照頁
1	インシデント発生時の初動対応フロー	混乱を最小化し、迅速な状況把握と対応を開始する。	[例]「発見者はネットワーク切断後、管理者へ電話報告。管理者が範囲特定後、緊急連絡先リストに基づき連絡。」	総務部 / ○○	P.65~66
2	重要システム・データ一覧と優先順位	業務継続に不可欠なシステムとデータの優先順位付け。	[例]最重要：受注、顧客マスター（RTO:4h, RPO:1h）。重要：生産管理（RTO:24h, RPO:1d）。	情シス担当 / ○○	P.30~33
3	代替手段・リカバリー手順	システム停止時の手動作業やデータ復旧手順を明確化。	[例]「受注は紙伝票で記録し、復旧後に一括入力。データ復旧はバックアップ手順に従い担当者が実施。」	各部門 / ○○	P.70, P.73~74
4	緊急連絡先リスト	社内・社外の主要な連絡先を網羅。	[例]「緊急連絡先リストを参照。掲示場所と責任者を明記。」	総務部 / ○○	P.66
5	復旧後の確認・検証事項	業務再開後のシステム・データの整合性、セキュリティ対策の確認	[例]「復旧後にデータ整合性とウイルス再スキャンを実施。原因調査報告書を作成し承認。」	情シス担当 / ○○	ー
6	BCPの訓練・見直し計画	定期的な訓練と見直しで実効性を高める。	[例]「年1回の訓練を実施し、結果を反映してBCPを見直す。」	総務部 / ○○	P.67~69

この簡易BCPは、事業を守る「最小限の羅針盤」です。訓練と見直しで実効性を高め続けましょう。

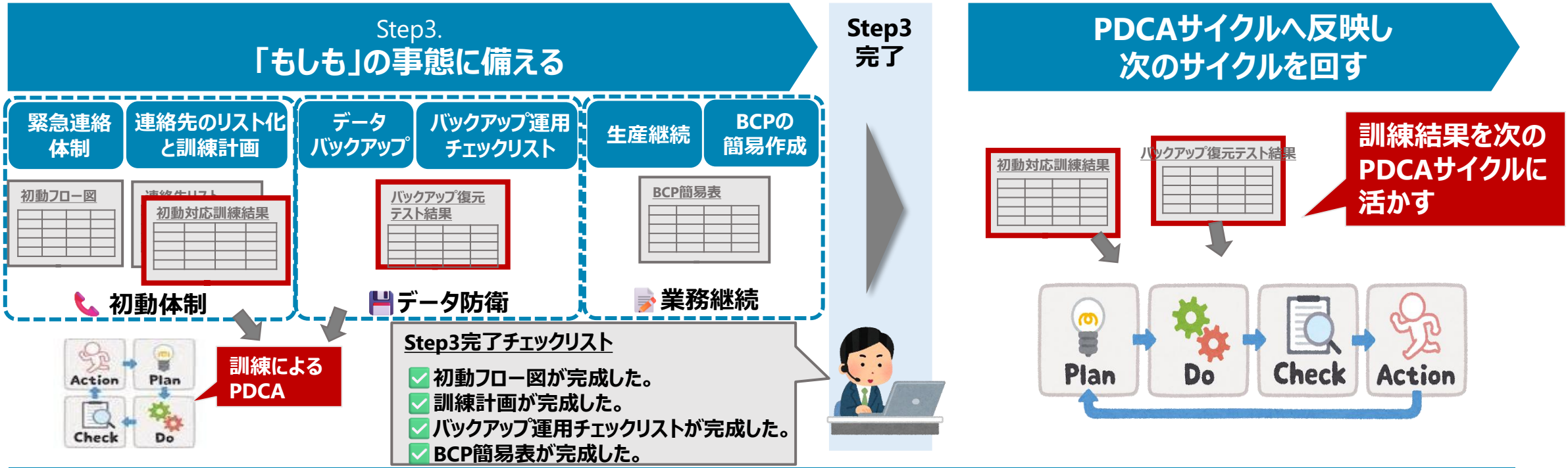
Copyright© Japan Automobile Manufacturers Association, Inc.

Step3の完了と次のアクション



対策の土台が完成　最大の山場を越え、実務的な防御に移る

- Step3の完了をもって、基本的な「事故発生時の対応」の基礎が固まりました。
  最後に、すべての備えが機能する状態にあるかを最終確認します。



次のステップは「実行」です。リストの優先度に基づき、すぐにアクションを開始しましょう。

Copyright© Japan Automobile Manufacturers Association, Inc.

6. 付録１ ユーザー企業4社の成功事例紹介

本付録では、実際に自動車産業のサプライチェーンで活躍されている中小企業4社への詳細なインタビューに基づき、セキュリティ対策の「生の声」をご紹介します。

「経営層の理解」「推進体制の構築」「予算確保」など、中小企業が直面する共通の課題に対し、各社がどのような工夫を凝らし、対策を進めてきたのか。具体的な取り組みや苦労、そこから得られた教訓を、それぞれの企業の従業員規模や背景とともにまとめました。

これらの事例は、机上の空論ではなく、皆様と同じ立場の企業が実践し、成功に至った確かな道筋です。
「自分たちにもできる」という気づきと、「次の一歩」を踏み出すための具体的なヒントが、ここにあります。
ぜひ、貴社の対策推進にお役立てください。

Copyright© Japan Automobile Manufacturers Association, Inc.

事例：Ａ社［従業員数：約150名］

経営層と推進リーダーが共にセキュリティ系に意識高く、自ら学びながらベンダーを活用し、対策を推進

- **人に恵まれた環境とセキュリティ意識の高さ:**
  - **社長はもともとセキュリティへの意識が高い。Web講習にも一緒に参加**する機会を作り、毎年**なぜこれだけ費用をかける必要があるか**理解
    ✅サイバー攻撃で被災したらもっと大変！ということを他社の被災例などから刺さるように説明。商品が品薄になり他社に客が流れるなど、会社経営悪化を伝え、危機感をあおった
  - **推進担当2名はもともとPCやネットワークが好きな人材**を充てている。好きで知っているからこそベンダーをうまく使っている。
    ✅社内でPCが好きなヒトを探し、情報交換する場を設けるなど、楽しんで推進できる環境を作って推進している
    ✅ベンダーに丸投げせず、担当者自身で試行錯誤し、新規導入ソフトの可否を判断している

- **BCP（事業継続計画）との連携:**
  - **東日本大震災の経験**から、**BCP（事業継続計画）の一環**としてセキュリティ対策に取り組んでいる点が特徴。
    ✅一度間違えてデータを消したことがある。データセンターまで出向き、入館手続きに苦労しながらもデータを引き抜いて持ち帰り復旧⇒特急の対応手順は理解・経験できた
  - セキュリティ対策をBCPの一部として捉えることで、**事業継続という観点からセキュリティの重要性を認識**し、対策を推進している。
    ✅推進体制は各課から人員を選出して分担。BCPがあるから受け入れられた。万が一の事態に備え、普段使用している画面を印刷して紙で準備。システム切替作業を活用して確認

- **EDRと資産管理ソフトの活用と入口・出口対策:**
  - EDR（Endpoint Detection and Response）と資産管理ソフトを導入。EDRで不審な動きを検知し、**PCの状況把握と迅速な対応**に役立てている。
  - ゲートウェイ装置はリモートにも対応可能。**入口と出口の監視**を重視し、診断ツールも活用。VPNが遅くなるが安全を優先。

- **社員教育や啓蒙活動:**
  - **攻撃型メール訓練（不定期）、セキュリティ教育の実施、社内インフォメーション、日々の通知啓発、会議体での説明**を実施
    ✅セキュリティに興味や知識のない従業員には、実際に触ってもらう・疑似体験をさせるなどの理解を促す工夫をしている
    ✅ランサムウェア被害の事例を出し、「みんな対策している」と横並び意識をあおるとよい

Copyright© Japan Automobile Manufacturers Association, Inc.

事例： B社［従業員数：約200名］

セキュリティ対策の重要性を早くから認識し、経営層の理解を得ながら、現場に負荷をかけずに対策を推進

- **経営層の巻き込みと意識改革:**
  - 経営層の理解を得るためには、**マクロ視点・外圧・ミクロ視点**など複数からアプローチするとよい
    - ✅マクロ：社外的な立場としてサイバーセキュリティ対応しないと社会的な信用を失墜してしまう
    - ✅外圧：官庁や親会社、取引先からの要請があったり、褒められると効果的
    - ✅ミクロ：ウイルス感染すると日々の業務が止まってしまう（例：メールが来ない/出せない、顧客向け資料を印刷できない）
  - 予算取りは**大きな数字を出さずに小出しにする。**PCの必須ソフトとして最初から一緒に予算取りするなど工夫して確保
    - ✅例）PC一台当たり1か月〇〇円 × 必要台数（内訳：PC本体、CS対策ソフト代…）
  - 経営層向けには脅すのでなく、「**従業員の皆さんを守る**ために必要な措置」「**自分が損しない**対応」「**従業員任せにせず**にシステムで守る」などの言い方が響いた

- **現場レベルでの意識向上とルール徹底:**
  - 従業員に対しても、**従業員自身が得になること**であることを訴求してセキュリティを進めた。
    - ✅出来ないことを前面に出さず、出来る範囲であれば自由にできることを強調
    - ✅例）「申請は出しておいた方が得だよ。社長承認を取っておけば安心して進められるよ！」「ルールを守った方が得だよ」
      「会社は、安全で守られているサイトだけ接続できるように接続しているよ」「止めているサイトも、業務に必要であれば、申請してもらえば通すから」
  - PC配布時に誓約書を提出させることで責任感を促し、インシデント発生時の報告義務を徹底している。

- **ガバナンス体制:**
  - 折々で**経営層から「セキュリティ責任者の言うことを聞くように」と発信**してもらい、セキュリティ推進者を公的に後押し
    - ✅各部署内のキーマンを味方にしながら推進。部門責任者をセキュリティ推進責任者に任命し、上と下から推進
  - 情報システム部門がセキュリティ対策を**一元管理**し、**作業者任せにしない**体制を構築。
    - ✅性悪説ベースの考え方に基づき、ツールを用いた徹底制御を実施。「使う人が容疑者にならないために」という考え方は共感を得られた

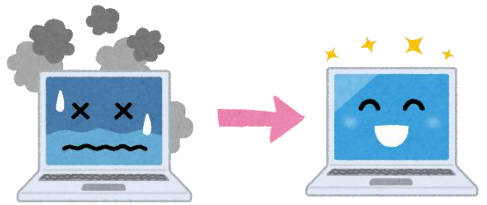
Copyright© Japan Automobile Manufacturers Association, Inc.

事例：C社［従業員数：約150名］

経営層の理解とリーダーシップの下、早期からセキュリティ対策を強化

- **製品特性と情報管理:**
  - 創業当時から作り方にノウハウがある商品を出していることから、**技術ノウハウがいかに重要かを身をもって理解**している。
    ✅従業員にも顧客情報だけではなく自社の図面情報も徹底管理するところは浸透している。情報を守る意識がしっかりしていることから、セキュリティにも取り組みやすかった
    ✅他社事例がいろいろあっても、自社の特徴を理解することが重要！
- **経営層のIT理解と独自のセキュリティ体制：**
  - **社長自身情報システム分野の経験者**だったこともあり、ITやセキュリティの重要性を深く理解し、**自ら推進**してきた。
  - 1998年自動車Tier1と取引を開始し、図面も**OEMとやり取り**することからセキュリティ対応の強い要請が来たことから対応を始めた。
  - 社長+2~3名の少人数体制で全社セキュリティを担当。他部署に担当を置かず、全ての問合せをこのチームで一元化している。

- **低コストで効果的な対策:**
  - **利便性よりコスト・信頼性を重視**
    ✅Wi-Fi環境の撤去、リモート接続やスマホ接続を基本禁止とすることで、追加対応コストを低減。監査対応やPC管理工数の削減に役立っている
    ✅ベンダー任せにせず、自分たちでできることは自分たちで行い、より安価で効果的な方法を常に模索している。追加投資よりも現状の運用見直しや効率化を重視
  - **情報システム部門による一元管理**
    ✅トラブル防止の観点から、重要システムの認証情報は情報システム部門が管理している
    ✅従業員からの相談やトラブル対応は、まず情報システム担当に連絡するルールを徹底



- **ガイドラインの活用と現実的な対応:**
  - Tier1から提示されたチェックリストに基づき、優先付けしてベンダーと調整してセキュリティ対応を推進。
    ✅動向調査よりも、チェックリストが最低ラインと理解して対応することが非常に有効。ただし、ガイドラインは大企業向けで抽象的な部分もあるため、現実的な落としどころを検討している

Copyright© Japan Automobile Manufacturers Association, Inc.

事例：D社［従業員数：約250名］

サイバー攻撃による被災から、経営層の理解と投資・地域連携の重要性を痛感

- **サイバー攻撃からの教訓:**
  - **サイバー攻撃による被災**が本格的な対策に取り組むきっかけ。**生産停止に対する影響度が計り知れないことを痛感。**
    ✅被災時は、生産現場での稼働が止まり、いつモノを出せるかも分からず、本当に苦しかった。生産現場は統率をとるのがすごく大変だった。
    ✅お客様にも影響が及んでしまった。寝れなかったり食事も喉を通らなくなり、精神的にも辛かった。

- **具体的なセキュリティ対策:**
  - **EDR導入**を最優先に、メールセキュリティ強化、FW※変更を実施。SOC※やNDR※の導入も視野に入れ、セキュリティ体制を強化。
    ✅メールセキュリティの導入により、スパムメールの多さを実感。自分達が置かれている環境とセキュリティ対策の必要性を再認識した。
  - 被災直後から、地域で情報交換会に参加し、**人脈作りと情報交換**を積極的に実施
    ✅地場の大手メーカーともつながりを持ったり、何十年もセキュリティを担当しているセキュリティに詳しい方とも知り合えて、問合せできるように。
- **経営層の巻き込みと投資判断:**
  - サイバー攻撃を実際に被災したことで、経営層の危機感が高まり、セキュリティ対策の必要性を強く認識するようになった。
    ✅経営層への説明では、「生産停止」や「情報漏洩」など、事業継続に直結するリスクを“見える化”して伝えた。
    ✅操業停止による被害コストの提示や、取引先・顧客への迷惑などを説明。
  - 予算は、セキュリティベンダーからの提案を基に、**松・竹・梅の3段階の案**を提示し、経営層に選択してもらった。

- **組織体制と人材育成:**
  - **セキュリティ委員会を経営層直下に設置**し、複数部門からメンバーを選出。
  - 社内のリテラシー向上を重視し、**教育・啓発活動**（情報セキュリティ月間、訓練、定期的な資料配布など）を継続的に実施
- **その他:**
  - **自動車産業サイバーセキュリティガイドライン**が対策の優先順位付けや具体的な実施策に役立つと評価。特に防御、バックアップ、情報漏洩防止に注力。

※FW：Fire Wall　※SOC：Security Operation Center　※NDR：Network Detection and Response

Copyright© Japan Automobile Manufacturers Association, Inc.

7. 付録２ 自動車産業サイバーセキュリティガイドラインとの関係

本付録では、自工会・部工会が策定している「自動車産業サイバーセキュリティガイドライン」の中から優先的に取り組むべき内容19項目を選定した「セキュリティ推進担当者向け解説資料 ～自動車産業サイバーセキュリティガイドライン 優先項目の解説～」（https://www.jama.or.jp/operation/it/cyb_sec/docs/cyb_sec_guideline_Security_Promotion_Handbook.pdf）にて取り上げている優先項目と、本手引きの記載項目との関係を整理しました。
「自動車産業サイバーセキュリティガイドライン」の「関連項目No.」とも対応付けていますので、参考にしてください。

Copyright© Japan Automobile Manufacturers Association, Inc.

優先的に対処すべき8項目と手引きとの対応①

自動車産業サイバーセキュリティガイドラインの中から優先的に対応すべき項目を抜粋したものと本手引きとの対応表

優先的に対応すべき項目		自動車産業サイバーセキュリティガイドライン		手引き	
分類	優先項目	関連項目No.	達成条件	頁	タイトル
1.セキュリティ事故発生時の構え	① 緊急時の対応手順や連絡体制の再確認	No.18	情報セキュリティ事件・事故発生時の対応体制とその責任者を明確にしていること	66 67 68 69	連絡先のリスト化と訓練計画① 連絡先のリスト化と訓練計画② 連絡先のリスト化と訓練計画③ 連絡先のリスト化と訓練計画④
		No.19	発生した情報セキュリティ事件・事故対応が実施され、事故の概要や影響および対応内容の記録がある		
		No.20	定期的、または必要に応じて、事故時の体制を見直ししている		
		No.24	情報セキュリティ事件・事故時の対応手順(初動、システム復旧等)を定めている	65	緊急連絡体制：初動フロー図
		No.26	マルウェア感染時の対応手順を定めている		
	② ネットワーク外でのバックアップ、データ保管	No.148	適切なタイミングでバックアップを取得している	70 71 72	データバックアップ：手順と重要性① データバックアップ：手順と重要性② バックアップ運用手順チェック
		No.149	復元(リストア)手順を整備している		
	③ サーバーダウン時の生産継続方法の検討	No.150	システムが停止した際も業務が遂行できる代替手段を用意している	73 74 75 76	生産継続：サーバーダウンに備える① 生産継続：サーバーダウンに備える② BCP（事業継続計画）の簡易作成① BCP（事業継続計画）の簡易作成②

Copyright© Japan Automobile Manufacturers Association, Inc.

優先的に対処すべき8項目と手引きとの対応②

自動車産業サイバーセキュリティガイドラインの中から優先的に対応すべき項目を抜粋したものと本手引きとの対応表

優先的に対応すべき項目		自動車産業サイバーセキュリティガイドライン		手引き	
分類	優先項目	関連項目No.	達成条件	頁	タイトル
2.侵入・拡散させない対策	① 脅威や攻撃手口の情報収集	No.16	サイバー攻撃や情報漏えいの新たな手口を知り、対策を社内部署へ共有している / サイバー攻撃や予兆を監視・分析をする体制を整備している	24 25	脅威情報：収集と活用方法① 脅威情報：収集と活用方法②
	② OS、ソフトウェアの最新版へのアップデート	No.124	情報システム・情報機器、ソフトウェアへセキュリティパッチやアップデート適用を適切に行っている	51 52 53	ソフトウェア最新化：緊急性① ソフトウェア最新化：緊急性② アップデートの運用手順チェック
	③ ウィルス対策ソフトの導入	No.136	パソコン、サーバーには、マルウェア感染を検知・通報するソフトウエア(ウイルス対策ソフト)を導入している	54 55 58	ウイルス対策ソフト：導入の基本① ウイルス対策ソフト：導入の基本② ウイルス対策ソフトの運用手順チェック
		No.137	ウイルス対策ソフトのパターンファイルは常に最新化している	56 57 58	導入後の運用とパターンファイル① 導入後の運用とパターンファイル② ウイルス対策ソフトの運用手順チェック
	④ パスワードの強化	No.115	パスワード設定に関するルールを定め、周知している	43 44 45	パスワード強化が必要な理由 パスワードの使いまわしを回避する方法 パスワード管理の運用チェックリスト

Copyright© Japan Automobile Manufacturers Association, Inc.

優先的に対処すべき8項目と手引きとの対応③

自動車産業サイバーセキュリティガイドラインの中から優先的に対応すべき項目を抜粋したものと本手引きとの対応表

優先的に対応すべき項目		自動車産業サイバーセキュリティガイドライン		手引き	
分類	優先項目	関連項目No.	達成条件	頁	タイトル
2.侵入・拡散させない対策	⑤ 共有設定の見直し	No.49	人の異動に伴うアクセス権(入室権限やシステムのアクセス権)の管理ルールを定めている	46 47 48 49 50	アクセス権限：制限の原則① アクセス権限：制限の原則② アクセス権限の適切な管理① アクセス権限の適切な管理② アクセス権限の適切な管理③
		No.51	管理ルールに沿ってアクセス権の発行、変更、無効化、削除を実施している		
		No.52	アクセス権の棚卸を定期的、または必要に応じて実施している		
		No.76	自組織の資産が接続している外部情報システムの利用ルールを定めている	59 60	【コラム】クラウド利用の注意点① 【コラム】クラウド利用の注意点②
		No.77	利用している外部情報システムを一覧化している		
		No.78	外部情報システムの一覧を定期的、または必要に応じて見直ししている		

Copyright© Japan Automobile Manufacturers Association, Inc.