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

一般社団法人
日本自動車工業会

一般社団法人
日本自動車部品工業会

2024年11月

目次

１．はじめに

サイバー攻撃者は常に弱い部分を狙っており、サプライチェーンの中で対策が遅れている企業を足掛かりに攻撃を拡大するなど、自動車産業を取り巻くサイバーセキュリティリスクは日々深刻化しています。
この様な環境の中で、安全・安心で豊かなモビリティ社会と自動車産業の持続可能な発展を実現するために、自動車産業に関わる一社一社自らが、サイバーセキュリティリスクに真摯に向き合い、適切な対処を行うことが必要不可欠です。

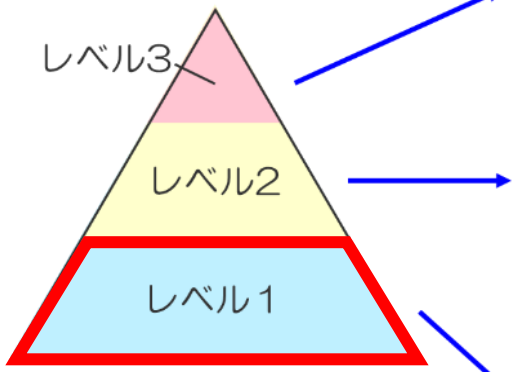
そのため、自動車メーカーやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した対策フレームワークや業界共通の自己評価基準を明示することで、自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的として、日本自動車工業会(JAMA)、日本自動車部品工業会(JAPIA)が共同で、**「自動車産業サイバーセキュリティガイドライン」**を2020年3月31日に初版策定しました。

業界推奨として、このガイドラインに於けるレベル２を目指した取り組みをお願いしておりますが、企業規模によっては、サイバーリスクから身を守る為に最低限度となるレベル１(50項目)の取り組みに対しても対応する事は困難であり、優先度をつけて行いたいとのご相談がありました。そこで、優先的に取り組むべき内容を「１.セキュリティ事故発生に備えた構え：3つの対策(8項目)」「２.侵入・拡散させない基本のセキュリティ対策：5つの対策(11項目)」にて整理させて頂きました。

※但し、この「8+11項目だけ」対策すれば良いと言う事ではなく優先度をつけた上でレベル２を目指した活動を行ってください。

2. 本書の位置づけ

ガイドラインは全体で153項目（Lv1: 50項目、Lv2: 74項目、Lv3: 29項目）で構成し、**Lv1 を自動車業界として最低限実装すべき項目**としています。本書はLv1を取り組むにあたりどこから取り組んだら良いか不安に感じる企業様に向けて、昨今のセキュリティ事故の状況を踏まえ、まずは優先して取り組むべき内容として「 セキュリティ事故発生に備えた構え」と「攻撃者やマルウエア等の侵入・拡散をさせない基本のセキュリティ対策」についてLv1の項目にそって具体的に解説するものです。



まず優先して取り組むべき内容を抽出

レベル	定義	各レベルの達成を目指すべき会社	
Lv3	現時点*で自動車業界が到達点として目指すべき項目 *2022年4月	・会社規模・技術レベルの観点で自動車業界を代表し牽引すべき立場の会社またはそれを目指す会社 ◆Lv1～3の全項目を達成	２９ 項目
Lv2	自動車業界として標準的に目指すべき項目	以下のいづれかに該当する会社 ・サプライチェーンにおいて社外の機密情報（技術・顧客情報等）を取り扱う会社 ・自動車業界として重要な自社技術／情報を有する会社 ・相応の規模／シェアを有し、不慮の供給停止等により業界のサプライチェーンに多大な影響を及ぼし得る会社 ◆Lv1,2の全項目を達成	７４ 項目
Lv1	自動車業界として最低限、実装すべき項目	・自動車業界に関係する全ての会社 ◆Lv1の全項目を達成	５０ 項目

1．セキュリティ事故発生に備えた構え 3つの対策（8項目）
2．侵入・拡散させない基本のセキュリティ対策 5つの対策（11項目）

3. 優先的に対応すべき項目（1／2）

分類	優先項目	目的	説明	自動車産業ガイド関連項目No.(Lv1)
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	セキュリティ事故発生時に早期に対応して、被害を最小化する	セキュリティ事故発生時には、対応すべき事が多岐にわたるため、事故が発生してから整理、準備していては時間が掛かってしまい、被害が拡大してしまいます。 セキュリティ事故対応では、必要な判断・対応を速やかに実施して、被害を最小限に留めるために対応手順、判断基準、報告先や報告内容を事前に明確にして、ドキュメント化しておくことが重要です。	No.18,19,20,24,26
	② ネットワーク外でのバックアップ、データ保管	被害を受けた際でも重要データは消失させない	データ暗号化やシステム破壊でデータが消失してしまった場合、業務復旧するためには手間とコストが膨大にかかり、事業存続にも影響が出る可能性があります。また、最近では、同一ネットワークに保管してあるバックアップデータを、暗号化される事例も発生しています。 データが消失した場合でも、早期復旧を可能とするために欠かさずバックアップを取得することと取得したバックアップはネットワーク外に保管しておくことが重要です。	No.148,149
	③ サーバーダウン時の生産継続方法の検討	システムが利用出来なくても生産／納入を継続させる	セキュリティ事故によってシステムが停止してしまうと、業務そのものの停止に繋がり、自社の利益を失うとともに取引先の利益にも影響を出してしまい、信用失墜や取引停止となることもあります。 事前に代替コミュニケーション手段やシステムを利用しない形での業務継続手段を明確にしておくことが重要です。	No.150

3. 優先的に対応すべき項目（2／2）

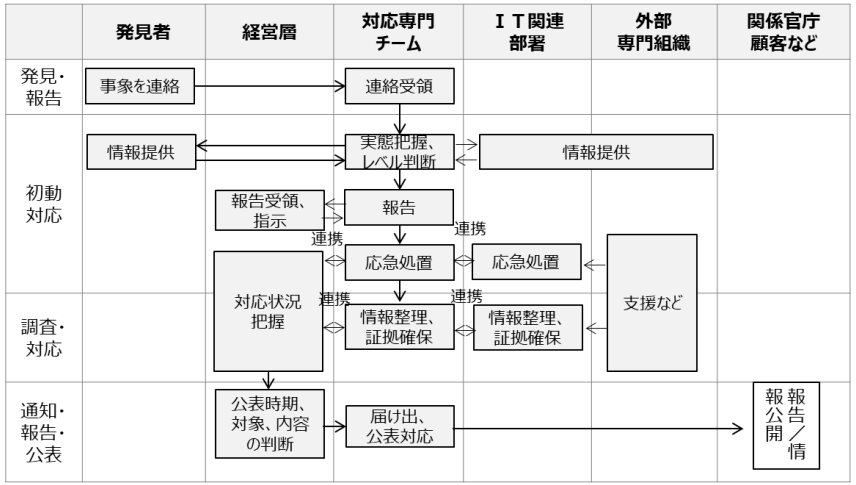
分類	優先項目	目的	説明	自動車産業ガイド関連項目No.(Lv1)
2. 侵入・拡散させない対策	① 脅威や攻撃手口の情報収集	脅威や攻撃手口の最新情報を知り、対策を検討する	攻撃者がどのような手口で攻撃するのか、他社で発生した攻撃事例はどのような内容なのか、情報を収集することで、どのような対策を取れば良いのか理解することが出来ます。 収集した情報を基に自社のセキュリティ対策を検討することが重要です。	No.16
	② OS、ソフトウェアの最新版へのアップデート	脆弱性を悪用した不正侵入を防止する	OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、 それを悪用した攻撃を受けてしまいます。 使用中のOSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用する事が重要です。	No.124
	③ ウィルス対策ソフトの導入	ウィルス感染によるデータ暗号化、不正侵入を防止する	ID、パスワード搾取やデータ暗号化といったウィルス感染は、依然として数多く発生している状況です。すべての端末にウィルス対策ソフトを導入し、最新のウィルスに対応できるようにパターンファイルは常に最新の状態にしておくことが重要です。	No.136,137
	④ パスワードの強化	パスワード推測、解析、窃取による不正アクセスを防止する	攻撃者は、よく使われるパスワードや桁数が少ないパスワードを総当たりで使い不正アクセスを試みます。また、同じパスワードを複数のクラウドサービスで使い回していると、1つのサービスで流出したIDとパスワードから不正アクセスを許してしまいます。 パスワード は「長く」「複雑に」「使い回さない」ことが重要です。	No.115
	⑤ 共有設定の見直し	誤設定による情報漏えいを防止する	クラウドサービスのアクセス権の設定不備でインターネット上の不特定多数から情報にアクセス出来てしまう情報漏えいの事例が増加しています。 クラウドサービスや社内機器の共有設定は、必要な人のみがアクセスできるように設定することが重要です。	No.49,51,52,76,77, 78

４．各項目解説
１-① 緊急時の対応手順や連絡体制の再確認

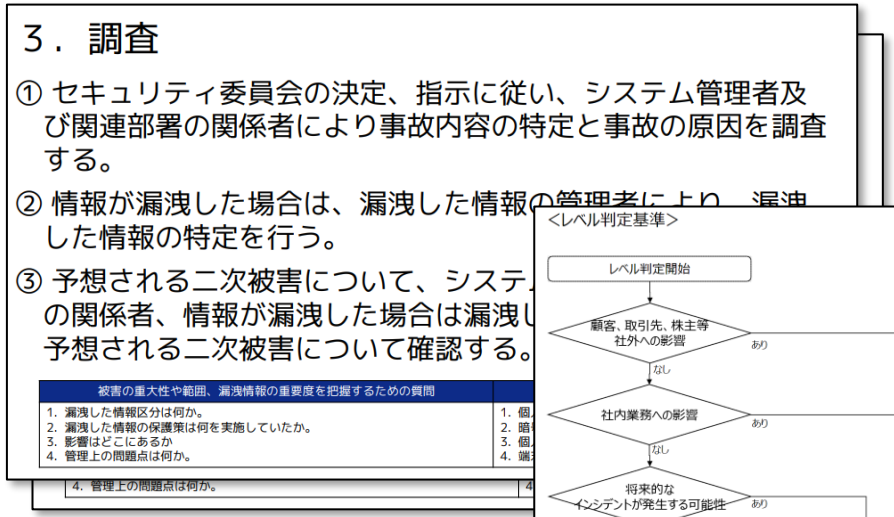
目的：セキュリティ事故発生時に早期に対応して、被害を最小化する

・セキュリティ事故対応の流れ及びその対応手順を予め明確にし、対応手順書と報告書ひな形、連絡先窓口一覧表を用意
　⇒役員を含めて社内全員に展開します

１）インシデント対応フロー（例）

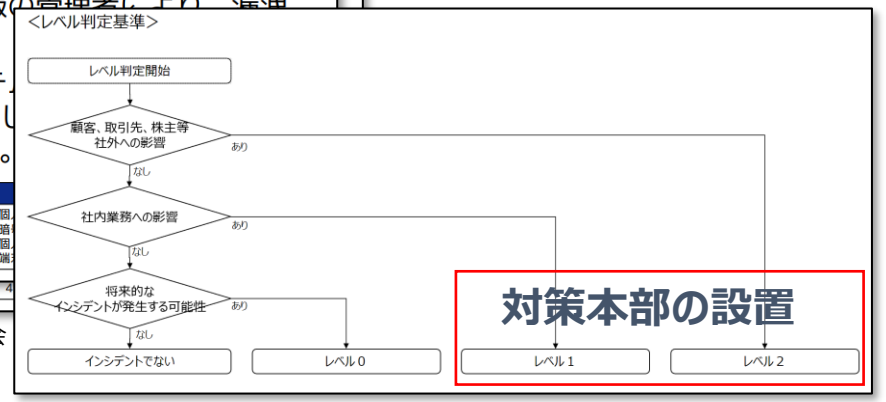


２）緊急時の対応手順書（例）



（出典）公益社団法人 私情協セキュリティ研究講習会

３）レベル判定基準（例）



<参考資料>

（出典）IPA ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄ対応手引き

中小企業のためのセキュリティインシデント対応の手引き　概要説明資料 (ipa.go.jp)

中小企業のためのセキュリティインデント対応の手引き (ipa.go.jp)

自動車産業ガイド 関連項目　No.１８、No.１９、No.２０、No.２４、No.２６

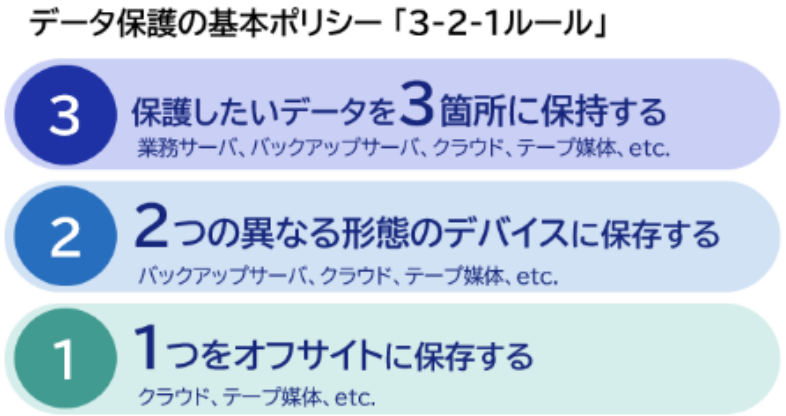
４．各項目解説
１-② ネットワーク外でのバックアップ、データ保管

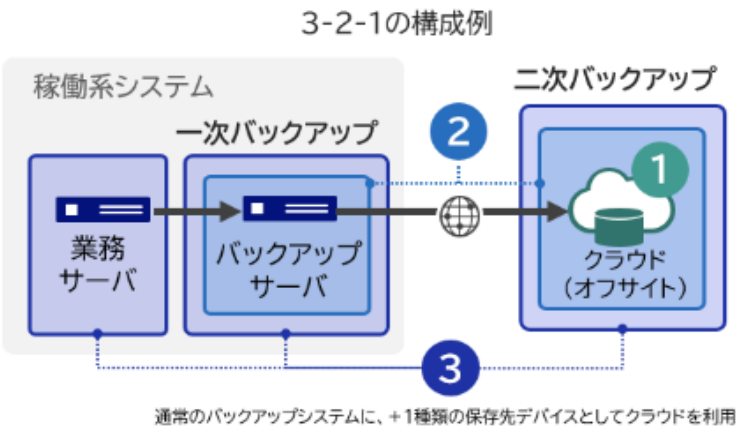
目的：被害を受けた際でも重要データは消失させない

- ビジネス影響を考えてバックアップするデータを決める
  対象例：基幹システム、顧客情報など
- どれくらいの頻度でバックアップを取るかを決める
  頻度例：データは日次、システム設定情報は月次など
- 保管先（バックアップサーバ、外部記録媒体、クラウド等）を決める

- 出来るだけ「3-2-1ルール（下図）」に則ろう
- バックアップソフト(※)等で自動化/効率化
  （信頼できる外部サービスを使う手も）
- 復元手順の整備も忘れずに

(※)参考 JNSAソリューションガイド

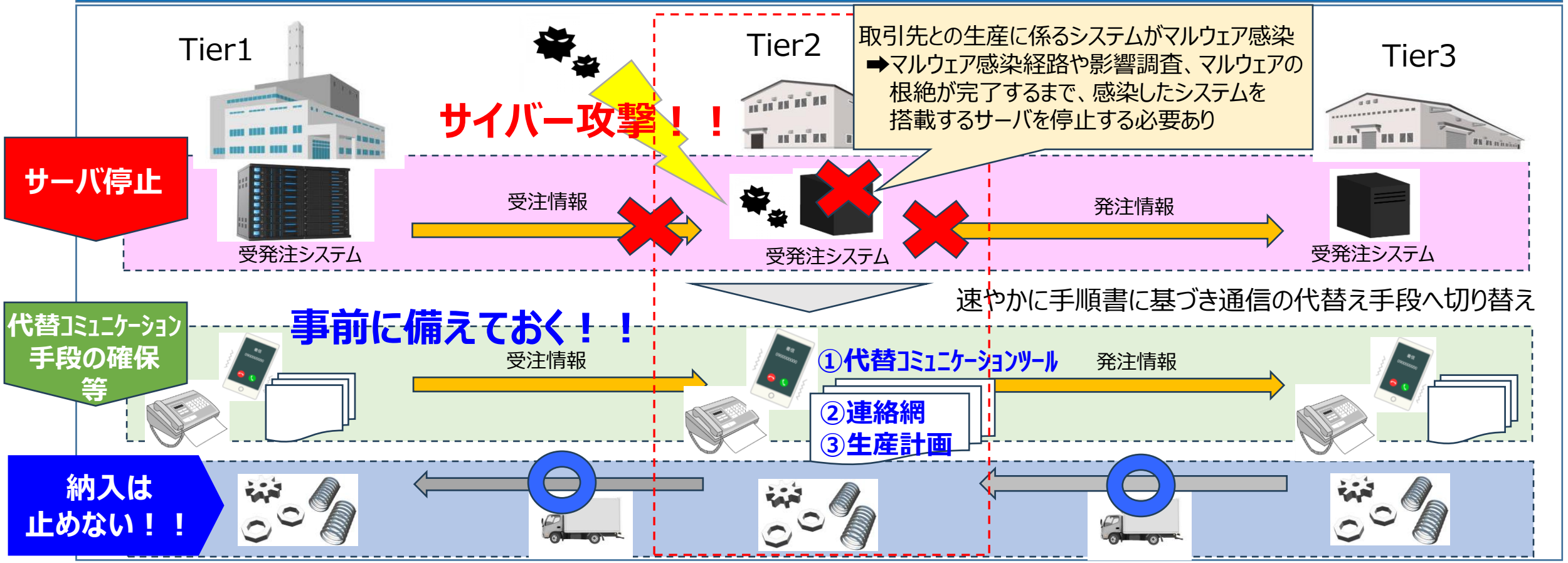




自動車産業ガイド 関連項目　No.148，No.149

４．各項目解説
１-③　サーバダウン時の生産継続方法の検討

目的：システムが利用出来なくても生産／納入を継続させる



自動車産業ガイド 関連項目No.150

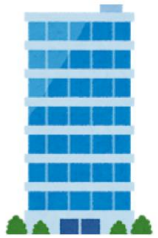
4．各項目解説
2-① 脅威や攻撃手口の情報収集

目的：脅威や攻撃手口の最新情報を知り、対策を検討する

・情報セキュリティに関する最新の攻撃手法や被害状況を定期的に把握し、自社の対策に反映させることで、類似のインシデントを防ぐことができる
・新たな手口を社内部署に共有することで、人為的ミス防止の注意喚起に繋げることができる

①定期的に(最低年1回以上)、以下に挙げたうち必要な情報源から情報セキュリティ事件・事故の事例、脅威、脆弱性などについて情報を得る

親会社や公的機関



ニュースレターなど

セミナー

・親会社からの通知
・公的機関(IPA等)のWebサイトを閲覧
・ベンダーのニュースレターに登録
・業界別セミナーに参加

②入手した情報を関係者に共有し、必要に応じて自社の対策を強化する

各職場内共有

eラーニング

啓発

左記“親会社からの通知”によって情報を収集する手段として、親会社が年次で開催するワークショップ等に参加し、必要な情報を得て、対策を実施している場合も可

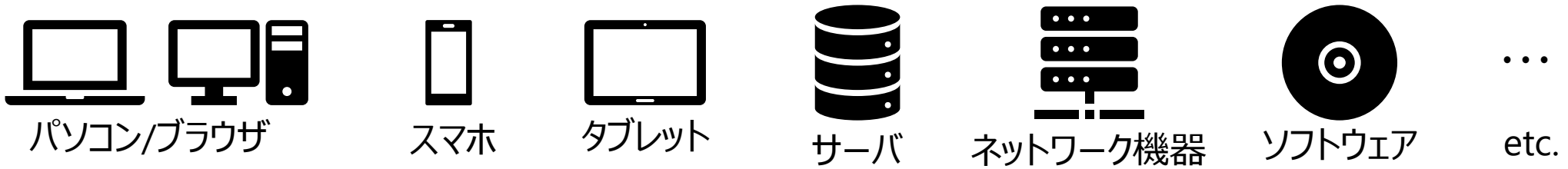
自動車産業ガイド No.16

４．各項目解説
2-② OS、ソフトウェアの最新版へのアップデート

目的：脆弱性を悪用した不正侵入を防止する

- OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、脆弱性を悪用した不正侵入のリスクとなります。お使いのOSやソフトウェアには、最新版のセキュリティパッチやアップデートが必ず必要になります。

➢ 多岐にわたる情報機器に対して、漏れなく適切にセキュリティパッチやアップデートを適用する



➢ セキュリティパッチやアップデート適用は、規則と期限を定め実施する

例）Microsoftの「緊急」レベルは即座に適用する、Windows Updateは毎月適用する　等

➢ パソコンにインストールされているソフトウェア製品が最新かどうかを以下のツールを使用して確認する

脆弱性対策情報共有フレームワーク - MyJVN

独立行政法人情報処理推進機構（IPA）のHPより

自動車産業ガイド 関連項目　No.124

４．各項目解説
２-③ ウィルス対策ソフトの導入

目的：ウィルス感染によるデータ暗号化、不正侵入を防止する

ウィルス対策は、サイバー攻撃から自社の情報資産を守るために、必須の対策です。
近年は、ランサムウェアと呼ばれる、コンピュータ内のファイルを暗号化する手口が増えています。

適切な対策を怠った場合、以下のような被害が想定されます。
・コンピュータ内のデータが暗号化され利用不可となり、身代金を要求される
・コンピュータ内の機密情報や個人情報が外部に流出する
・他組織へのサイバー攻撃の踏み台に利用される

万が一、自組織のコンピュータにウィルス対策ソフトが導入されていない場合は、早急に対策が必要です。
その際は、パターンファイルを常に最新化し、定期的にウィルススキャンを実行しましょう。

自動車産業ガイド 関連項目　No.136, 137

4．各項目解説
2-④パスワードの強化

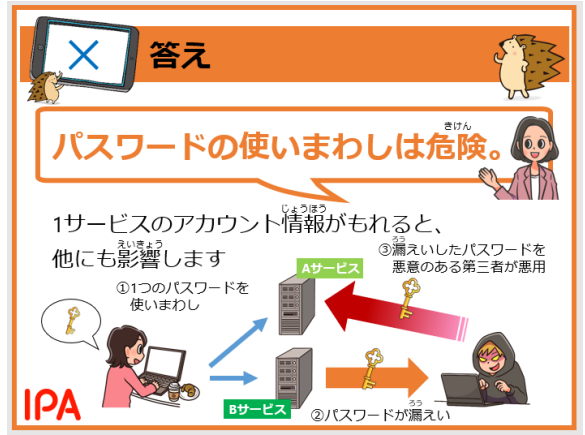
目的：パスワード推測、解析、窃取による不正アクセスを防止する

情報システムの不正利用や情報漏洩・改ざんを防ぐため、パスワード管理が重要です。
攻撃者は、よく使われるパスワードや桁数が少ないパスワードを総当たりで使い、不正アクセスを試みます。以下の取り組みを実施しましょう。

① パスワードに関するルールを定め、社内に周知徹底する。
《ルールの例》
・パスワードの桁数を8桁以上にする
・パスワードに使用する文字を英大文字、英小文字、数字、記号のうち3種以上を組み合わせる
・パスワードは使い回さない
・パスワードは90日で強制的に更新を促す設定にする

② パスワードに関する教育・啓発活動を行う。
独立行政法人情報処理推進機構（IPA）ホームページにパスワードに関する情報が多数掲載されています。これらを利用して、社内への啓発活動を実施しましょう。
一般初心者向け情報セキュリティ教材 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構
パスワードーもっと強くキミを守りたいー ： IPA情報処理推進機構

《IPA教材例》



自動車産業ガイド 関連項目　No.115

4．各項目解説
2-⑤共有設定の見直し

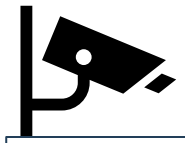
目的：誤設定による情報漏えいを防止する

・インターネットからアクセス可能なシステムの共有設定が間違っていたり、不要なユーザーアカウントが残っているとサイバー攻撃を受けて情報漏洩が発生してしまいます。無関係な人が、ウェブサービスや機器、システムを使うことができるような設定になっていないことを確認しましょう。

- インターネットからアクセス出来るシステムの共有は必要最低限にしましょう。
- 利用者一覧を作り、退職・異動した人はすみやかに削除・停止をしましょう。
- 定期的にユーザーアカウントの確認をしましょう。

- なるべく個人別のユーザーアカウントにしましょう。
- 共有設定の確認は年一回以上を目安に。
- パスワードの定期変更や二要素認証の利用も有効です。

業務システム



Webカメラ

共有フォルダ

クラウドシステム

・共有は本当に必要ですか？
・誰でも見れるようになっていませんか？
・パスワードは定期的に変えていますか？

Aシステム利用者一覧

ユーザ	権限	登録日
Nakao	管理者	2024/1/1
Yamamoto	一般	2024/2/3
Satou	一般	2024/3/3

重要なシステムはユーザ一覧を作りましょう。

Aシステム共有確認表

ユーザ	権限	登録日	必要
Nakao	管理者	2024/1/1	○
Yamamoto	一般	2024/2/3	×
Satou	一般	2024/3/3	○

不要なユーザが残っていないか定期的に確認をしましょう。

自動車産業ガイド 関連項目　No.49,51,52,76,77,78

５. まとめ

本書では、優先的に取り組むべき内容を

１．セキュリティ事故発生に備えた構え：3つの対策(8項目)
２．侵入・拡散させない基本のセキュリティ対策：5つの対策(11項目)

の8+11項目にて整理させて頂きました。
まずは、本書を参考にこの優先事項を確実に対応してください。

また、この優先事項は、最低限取り組むべきレベル１の中でも必須で取り組むべき項目である事をご理解いただき、優先度をつけた上で、**レベル２を目指した継続的な活動を行ってください。**

ご視聴ありがとうございました