規定コード	D-1-6-1

情報セキュリティーポリシー

九州日野自動車株式会社

基 本 方 針

1.目　的

当社の効率的で効果的な事業活動を継続的かつ安定的に確保するためには、適切な情報セキュリティー対策を実施して高度な情報セキュリティー水準を達成することが必要不可欠である。
このため､情報セキュリティ対策の包括的な基本方針として､本情報セキュリティーポリシーを策定し、当社の情報資産をあらゆる脅威から守るために必要な情報セキュリティーの確保に最大限取り組むこととする。

2.定　義

本ポリシーで使用する用語の定義は、次の通りである。

・情報セキュリティー
　情報資産の機密性、完全性及び可用性を維持すること。

・情報資産
　情報及び情報を管理する仕組み（情報システム並びにシステム開発、運用及び保守のための資料等）の総称。

・情報システム
　同一組織内において、ハードウエア、ソフトウエア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うもの。

・情報セキュリティーガイドライン（以下「ガイドライン」という。）
　当社が所有する情報資産の情報セキュリティー対策について､体系的かつ具体的に規定したもの。「どのような情報資産をどのような脅威から、どのようにして守るのか」についての具体的な方策を規定したもの。

3.対象範囲

本ポリシーの対象範囲は、当社が業務で使用するネットワーク、ハードウエア、ソフトウエア、記録媒体等の情報システム等（システム構成図等の文書を含む。）及びすべての情報のうち、情報システムに電磁的に記録される情報、並びにこれらの情報に接するすべての社員、準社員、外部委託事業者等とする。

（例）

対　　象	例
情報システム等	コンピュータ、基本ソフトウエア、応用ソフトウエア、ネットワーク、通信機器、記録媒体、システム構成図等
情報システムに記録される情報	文書及び図面等の電磁的記録、アクセス記録
これらの情報に接するすべての者	常勤、非常勤及び臨時を含む社員、外部委託事業者等

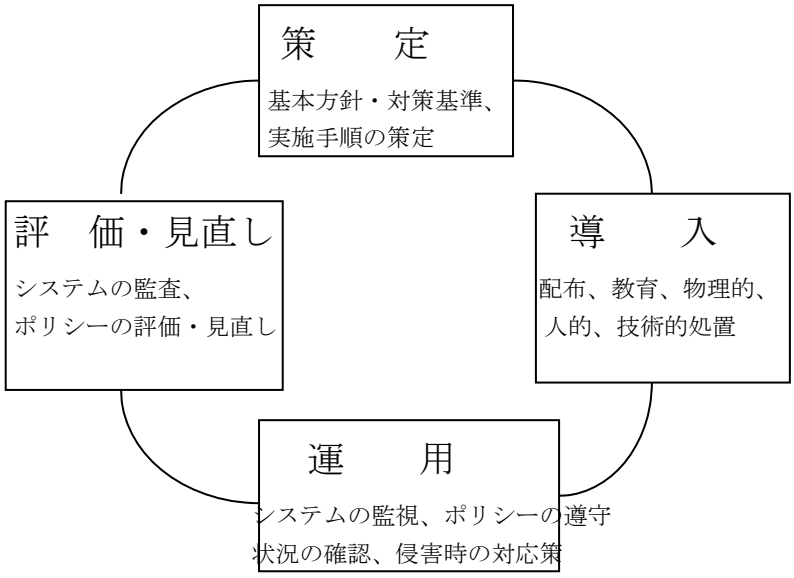
4.本ポリシーの基本的な考え方

・ IT の発展速度は極めて速いため、ある時に講じた最高の情報セキュリティ対策が、将来にわたっても最高のものとして永続することはない。その時々のハードウエア、ソフトウエアの導入は導入時には適切な情報セキュリティ対策であり得るが、継続性は保証されていない。
情報セキュリティー対策は、情報セキュリティーポリシーを策定することによって完結する一過性の取組みではなく､情報セキュリティーガイドライン等の策定　及びそれに続く日々の継続的な取組みによって確保される性質のものである。

・ このため、継続的な情報収集及びセキュリティー確保の体制を構築し、また「いかに破られないか」のみならず「破られたときどうするか」についての対策も適切に規定し、当該規定に基づいた対策を十分に構築する。

・ さらには､情報セキュリティーポリシー及びそれに関連するガイドラインを定期的に見直すことによって、当社の所有する情報資産に対して、新たな脅威が発生していないか、環境の変化はないかを確認し、継続的に対策を講じていく。
特に、情報セキュリティーの分野では、技術の進歩やハッカーの手口の巧妙化に鑑み、早いサイクルで見直しを行っていく。

情報セキュリティーポリシーの実施サイクル



著作権法、不正アクセス禁止法、個人情報保護法など情報セキュリティーに関連する法令、並びに業界のガイドラインなどを遵守するための措置を講じる。

情報セキュリティーの確保には、日野自動車（株）及び、情報システム所管部署だけでなく、
情報システムを利用する個々の一般ユーザーの努力も不可欠である。

このため、当社のすべての社員（常勤、非常勤及び準社員）は、本ポリシー及びガイドラインの実施に責任を負うとともに、ポリシーを尊重し、ガイドラインを遵守しなければならない。
本ポリシーは情報セキュリティーを確保するための基本方針であり、その方針は社員ユーザーに各種の制約を課することになるが、ポリシーの目的は業務の効率的で継続的かつ安定的な遂行にあることを忘れてはならない。
この点に関して一般社員の理解と協力を求めることに尽力するとともに、実態に即したユーザーの意見を反映できる仕組みを導入する。

情報セキュリティーに関して問題が発生あるいは予見された場合、本ポリシー及びガイドラインに基づいて対処する。
すなわち、一部関係者のみで秘密裏に処理することはあってはならない。
なお、予想される脅威に対して万全の策を講じるということは、厳格すぎるガイドラインを定めればよいという意味ではない。
危険性から完全隔離した無菌室状態しか経験していないユーザーは免疫機能が働かずに却ってリスクに脆弱な体質になってしまうことに留意する必要がある。

５.対策基準に関する基本方針

（１）組織・体制

情報セキュリティーの確保のための組織・体制は、役員が率先して推進することが重要であることから､情報セキュリティーについて最高責任者(セキュリティー管理担当責任者)を定める。
この最高責任者を長として､全社としてＩＴセキュリティー対策を推進するための組織・体制を定め、その責任及び権限を明確にする。

（２）情報の分類と管理

当社の情報システムにおいて取扱う情報について、重要な情報を重点管理する考え方から、重要度に応じた情報分類の定義、情報の管理責任、管理の方法を規定する。

（３）物理的セキュリティー

情報システムの設置場所について、不正な立入り、損傷及び妨害から情報資産を保護するため、管理区域を設置する等の物理的な対策を規定する。

（４）人的セキュリティー

情報セキュリティーに関する権限や責任を定め､すべての社員にポリシー及びガイドラインの内容を周知徹底する 等、十分な教育及び啓発が講じられるように必要な対策を規定する。

（５）技術的セキュリティー

当社の情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の必要な対策を規定する。

（６）運用

ポリシー及びガイドラインの実効性を確保するため､また､不正アクセス及び不正アクセスによって他の情報システムに対する攻撃に悪用されることを防ぐため、ポリシー及びガイドラインの遵守状況の確認、運用面に関して必要な措置を規定する。

また、緊急事態が発生した際の迅速な対応を可能とするため、緊急時対応処置を規定する。

（７）法令･社則の遵守

法令や社則、及び　セキュリティーポリシーとガイドラインの遵守について規定する。

（８）情報セキュリティーに関する違反に対する対応

法令･社則､セキュリティーポリシー及びガイドラインに違反した場合の罰則について規定する。

（９）評価・見直し

ポリシー及び情報セキュリティー対策の評価、新たな脅威等を踏まえ、定期的に対策基準の評価・見直しを実施することとし、このための必要な措置を規定する。

６.実施手順に関する基本方針

対策基準に定められた内容を具体的な情報システム又は業務において遂行していくために、具体的なガイドラインを作成し、その手順に基づいて対策を実行する。

付則

１．この規定の主管部署は、**総合企画部**とする。
２．この規定の改廃は、**総合企画部**が起案し、役員会の承認により行う。
３．この規定は、平成１８年１０月２４日より施行する。
４．この規定は、平成２１年　８月１１日より施行する。
５．この規定は、平成２９年　７月１０日より施行する。
６．令和　２年　５月２５日改定。