自動車リサイクルシステム

情報セキュリティ
基本方針書

文書作成責任　：情報セキュリティ部会

目　　次

第 1 章　総則

1.1　目的

「使用済自動車の再資源化等に関する法律」(以下、自動車リサイクル法という)に則り構築された自動車リサイクルシステムの運用に際し、自動車リサイクル運用委員会に参加する法人・チームは、自動車ユーザーの個人情報、車検証情報、リサイクル資源の引取・破壊に関わる事業情報などの情報資産(以下、情報および情報を取り扱う仕組みを「情報資産」とする)を取り扱う。社会的システムとしての信頼に応えるためには、情報資産を保護する情報セキュリティ対策は必須である。本基本方針書は、情報セキュリティ対策の基本的な方針を定め、情報資産の改ざん、漏洩および不正アクセスなどを防ぐことを目的とする。

1.2　定義

基本方針で用いる用語は、次の定義とする。

(1)情報セキュリティ

情報化・ネットワーク化の進展にともなって、情報の価値は飛躍的に高まっている。そのため、情報を他の事業資産と同じく重要な資産と考えて、情報資産を適切に保護する情報セキュリティ対策を講じることが不可欠となっている。

情報セキュリティとは、想定されるさまざまな脅威から情報資産の機密性、完全性および可用性を維持することとする。

情報資産への脅威には、大きく以下の3つがある。

①自然の脅威　　:地震、火災、風水害など
②人間の脅威　　:機密情報の持ち出し、パソコンの盗難、コンピュータの操作ミスなど
③システムの脅威　　:ハードウェアの故障、ソフトウェアの不具合など

情報資産は、以下の3つの側面から保護する必要がある。

①機密性　　:認可された利用者だけが情報資産にアクセスできること
(情報の漏洩を防ぐこと)
②完全性　　:情報資産の内容が正確であること
(情報が故意に改ざんされること、ミスにより変更されることを防ぐことなど)
③可用性　　:認可された利用者が、必要なときに、情報資産を利用できること
(外部からのシステムへの妨害、システムの故障などが発生したときにも、情報資産を利用できるようにすること)

情報セキュリティの保護対象は、電子的なデータはもちろん、コンピュータおよび記憶媒体、印刷物等の紙媒体、人の頭のなかにある情報、音声などを含めた、すべての情報および伝達手段とする。

(2)自動車リサイクル法

平成14年7月に「使用済自動車の再資源化等に関する法律」が成立し、平成17年 1 月に施行される。使用済自動車から出る有用資源をリサイクルして、環境問題への対応を図るための法律である。

参考ホームページ　http://www.meti.go.jp/policy/automobile/main_02.html

(3)公益財団法人自動車リサイクル促進センター

使用済自動車の処理を円滑化し、自動車リサイクルの一層の高度化を促進することを目的とし設立された組織であり、自動車リサイクル法上の指定法人である。略称は JARC(Japan Automobile Recycling Promotion Center)である。

参考ホームページ　http://www.jarc.or.jp/

(4)一般社団法人自動車再資源化協力機構

自動車製造業者等が行うべき使用済自動車のフロンならびにエアバッグ類の引取り及び再資源化等を共同して実施することを目的として設立された組織である。略称は自再協である。

参考ホームページ　http://www.jarp.org/

(5)ASR チーム

ASR(Automobile Shredder Residue:自動車シュレッダーダスト)を適正かつ確実にリサイクル・処理し、リサイクル率の向上を図るため、自動車製造業者等を2つのグループに分けた各々の組織である。

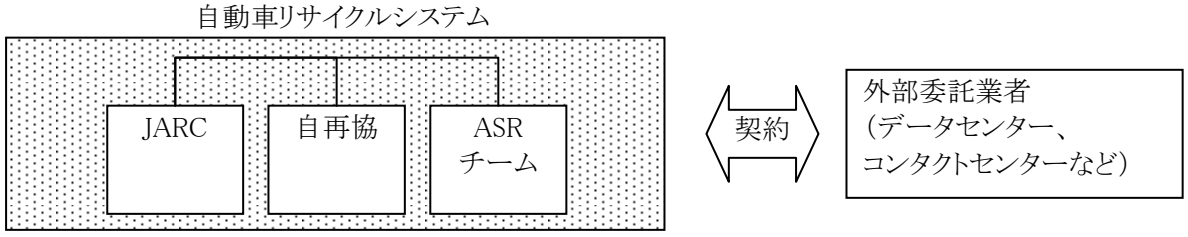
(6)自動車リサイクル運用委員会

自動車リサイクルシステムの構築、運用に関与する JARC、自再協、ASR チーム、一般社団法人日本自動車工業会で構成される委員会である。

1.3 適用範囲

情報セキュリティ基本方針の適用範囲は、自動車リサイクルシステムの情報資産を主体的に管理する JARC、自再協、ASR チーム、およびこれら組織の一部の機能を請け負う外部委託業者などとする。

尚、外部委託業者については、委託業務遂行に際し情報セキュリティ基本方針を含む情報セキュリティ規程に準拠する旨を外部委託に関わる契約書に記載するものとする。



1.4 情報セキュリティ規程体系

情報セキュリティ規程は、情報セキュリティ対策について、その目的・考え方から個別の管理方法・手順などを体系的に定めたものの総称である。情報セキュリティ規程体系は、「基本方針書」「対策基準書」「ガイドライン」の3階層からなり、以下に内容を示す。

(1)基本方針書

情報セキュリティの目的および基本的な考え方(方針)を定める。

(2)対策基準書

基本方針書に基づいた情報セキュリティの基本的なルールを定める。

(3)ガイドライン

基本方針書および対策基準書に基づいた具体的な管理方法や利用・運用の手続きなどをガイドラインとして別途定める。

第 2 章　情報セキュリティの基本方針

各法人・チームの情報セキュリティの継続的な維持・向上を図るために、日々変化するリスクや突発的な事象に対して適切なリスクマネジメントを行う。更に、情報セキュリティ対策が有効に機能していることを確認するために、情報セキュリティに関する監査を定期的に実施する。また、情報セキュリティ事故が突発的に発生した場合のことを考慮し、解決策の実施や回避策などを検討するための体制や対応手順を事前に明確にする。

2.1 情報セキュリティの管理体制

情報資産の活用方法が多様化していくなかで、情報資産の管理の手法も多種多様となっている。自動車リサイクルシステムにおける情報セキュリティを確立し、情報資産を適切に管理するために情報セキュリティの推進体制および責任体制を確立する。

2.2 情報資産の分類及び管理

情報は重要なものであれば、紙や電子情報といった媒体や保存方法に関わらず厳密に取り扱われなければならない。情報資産を適切に管理するために、情報資産をその重要度により分類し、重要度に応じた取扱い方法を定める。

2.3 人的情報セキュリティ

自動車リサイクルシステムの業務に携わる職員の情報セキュリティに対する役割と責任を定める。情報セキュリティ規程の適用対象者に対して、自身の役割と責任、実施すべき施策について共通認識を持つことができるように、適切な教育を実施する。また、採用時および退職時の職員の管理を適切に行う。

2.4 物理的セキュリティ

第三者による物理的な不正侵入や業務への不正な介入を防止し、情報資産を盗難や破壊から保護するために、建物やオフィスに対して適切な防護措置を行う必要がある。このため、各法人・チームの施設を重要度に応じたエリアに区分し、エリア毎に物理的な対策を講じる。

2.5 システムセキュリティ

業務機能の多くは、システムやネットワークを活用した情報処理に依存している。適正な業務の遂行を確保し、正しい業務処理を継続的に実施するためには、システムおよびネットワークの情報セキュリティの確立が不可欠である。このため、システムやネットワークの「運用管理」「開発」「利用」について、情報セキュリティ確保のための施策を講じる。

2.6 ビジネス継続管理

情報セキュリティ事件・事故、情報システム障害、自然災害等により自動車リサイクルシステムの情報資産の破壊や業務機能の停止などの可能性がある。速やかに復旧を行い業務を継続させることを目的にビジネス継続計画を策定する。ビジネス継続計画は、策定するだけでなく、それが正しく機能することを検証し、且つ時代や業務に適したものに改廃していく。

2.7 規程の遵守

健全な事業運営を遂行するために、法律や契約、情報セキュリティ規程を遵守する。