自動車リサイクルシステム

情報セキュリティ
対策基準書

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

自動車リサイクルシステムの情報資産に対する共通の取扱い方法及び情報セキュリティにおける基本的なルールを定める。なお、当対策基準書は、自動車リサイクルシステムにおける情報セキュリティの共通の管理レベルを示すものである。

1.2　適用範囲

情報セキュリティ基本方針書を参照のこと

1.3　当対策基準書の責任担当

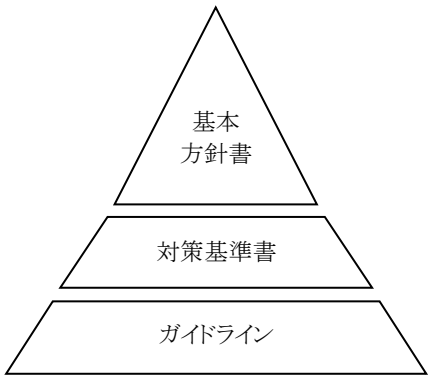
情報セキュリティ部会が責任担当として作成、改訂および発行を行う。

1.4　当対策基準書の関連文書

・情報セキュリティ基本方針書

1.5　本書の位置付け

情報セキュリティ規程は、情報セキュリティの国際標準規格「ISO/IEC17799（注）」に基づいて策定され、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をいう。自動車リサイクルシステムの情報セキュリティ規程は、「基本方針書」「対策基準書」「ガイドライン」の3階層から構成され、体系的に管理する。本書は、情報セキュリティ規程体系のなかの対策基準書とする。



情報セキュリティ規程体系

(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）を別途定める。

(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。

（注）ISO/IEC17799

情報セキュリティを管理する仕組みの国際規格として、ISO（国際標準化機構）と IEC（国際電気標準会議）がまとめた実践規範である。

第 2 章　情報セキュリティの管理体制

2.1　情報セキュリティ組織

全体最適の観点から情報セキュリティの維持、向上を図ることを目的に各法人・チームを横断する情報セキュリティ組織を整備する。情報セキュリティ組織は、情報セキュリティ責任者、各法人・チームの情報セキュリティ管理者、及び情報セキュリティ部会で構成する。

(1)情報セキュリティ責任者

各法人・チームの長を情報セキュリティ責任者とする。各法人・チーム内の情報セキュリティに関する全ての責任を有し、情報セキュリティ管理者の任命や外部に対する説明責任がある。

(2)情報セキュリティ管理者

情報セキュリティ管理者は、情報セキュリティ責任者が任命する。各法人・チーム内の情報セキュリティに関する推進責任を有する。

(3)情報セキュリティ部会

各法人・チームの情報セキュリティ管理者で構成する組織とし、自動車リサイクルシステム全体の情報セキュリティに関する事項の検討や課題解決を行う。以下にその役割と責任を示す。

・情報セキュリティ規程の策定、検討、更新を行う。
・情報セキュリティを普及啓発するために情報セキュリティ教育を行う。
・情報セキュリティ事件・事故に関するレビューと対策を検討する。

2.2　情報資産を保護するための役割と責任

情報資産を適切に保護することを目的に、「所有者」「提供者」「利用者」の3つに区分し、情報セキュリティに関する各々の役割と責任を明確にする。

(1)所有者

情報資産の所有者は、当該情報資産を生成した者である。以下にその役割と責任を示す。

・情報資産の利用者および利用範囲を定める。
・情報資産の使用目的および重要度を判断し、情報資産の分類や情報資産の取扱い方法を定める。
・情報資産の保護、及び管理する仕組みを策定し、「提供者」へ委託する。

(2)提供者

情報資産の提供者は、情報資産の運用管理を所有者から委託された者である。以下にその役割と責任を示す。

・情報資産を保護・管理する仕組み（文書・書類の保管や閲覧の許可、システムへのアクセス権限の設定など）の実装や適切な運用を行う。

(3)利用者

情報資産の利用者は、情報資産を利用し業務を遂行する者であり、情報資産の取扱い方法に従い利用する責任を有する。

第 3 章　情報資産の分類及び取扱い

3.1 情報資産の分類

情報資産の重要度に応じた管理を実施するため、情報資産を「機密性」「完全性」「可用性」の 3 つの側面から分類する。

(1)機密性区分

各法人・チームは情報資産を機密性の観点から最低限以下の 3 つに区分し、定めることとする。

機密性区分	説明	例
Ⅰ	情報を知りえる者のみに利用が限定された情報資産である。仮に漏洩した場合には重大な損害を被る可能性があり、厳格な機密保持を要する情報資産である。具体的には情報資産の開示範囲外への流出等漏洩時に以下の影響が想定されるもの。 1．　第三者から法的責任や損害賠償責任などを問われる。 2．　業務や職員に極めて大きな混乱が生じる。	人事情報 パスワード 契約書 など
Ⅱ	情報資産が漏洩した場合に損害を被るものであり、具体的には情報資産の外部への流出等漏洩時に以下の影響が想定されるもの。 1．　業務遂行に支障をきたす可能性がある。	内部文書 など
Ⅲ	機密保持の制限を要しないもの。 外部に広く公開されることを前提としているため、制限を設ける必要のない情報資産。	ホームページ情報 など

(2) 完全性区分

各法人・チームは情報資産を完全性の観点から最低限以下の2つに区分し、定めることとする。

完全性区分	説明	例
Ⅰ	情報資産が改ざんされた場合に、重大な損害を被るものであり、特別な完全性の確保を要するもの。 具体的には情報資産が改ざんされたり破壊されることにより以下の影響が想定されるもの。 1．　第三者から法的責任や損害賠償責任などを問われる。 2．　業務や職員に極めて大きな混乱が生じる。	契約書、 会計情報 など
Ⅱ	完全性の確保を要しないもの。 改ざんや破壊されても損失を受けることが少ないと判断されるため、制限を設ける必要のない上記区分以外の情報資産。	マニュアル など

(3)可用性区分

各法人・チームは情報資産を可用性の観点から最低限以下の2つに区分し、定めることとする。

可用性区分	説明	例
Ⅰ	情報資産が利用できない場合に、重大な損害を被るものであり、特別な可用性の確保を要するもの。 具体的には、情報資産を利用できないことにより以下のような損害を被ることが想定されるもの。 1. 第三者から法的責任や損害賠償責任などを問われる。 2. 業務や職員に極めて大きな混乱が生じる。	預託に関する情報、など
Ⅱ	可用性の確保を要しないもの。 情報資産を利用できない場合にも損失を受けることが少ないと判断されるため、制限を設ける必要のない上記区分以外のもの。	マニュアル等

3.2 情報資産の取扱い

情報資産の取扱いについては、情報資産の分類に応じて管理要件を決定し取扱い方法を定める。管理要件については、情報資産の利用サイクルや管理サイクル等の場面に応じた取扱い方法を考慮して、情報資産の取扱い方法を別途定める。

特に重要な情報資産については、所有者、区分、配置場所、形態等を明確にする。

第 4 章　人的情報セキュリティ

4.1　職掌上の役割と責任

自動車リサイクルシステムの業務に携わる者は、自身の役割と責任に自覚を持ち、情報セキュリティの重要性を理解し、職務を遂行する。情報セキュリティ確保のために、職掌上の役割と責任を定める。

(1)全職員（役職員、協力会社、派遣職員、パート、アルバイト）

全職員の役割と責任を以下に示す。

・情報セキュリティの重要性を理解し、定められた事項を遵守する。

・情報セキュリティの管理体制の中で自身の役割と責任を理解し、業務を遂行する。

・業務中はもとより、業務を離れた場合にも情報セキュリティ確保の責任を持つ。

・全職員は各法人・チームの業務に従事する際、事前に情報セキュリティ規程に従い、情報セキュリティを遵守する旨の同意を示すため、適宜、法人・チームとの間で同意書を取り交わす。

(2)情報セキュリティ責任者／情報セキュリティ管理者

情報セキュリティ責任者／情報セキュリティ管理者の役割と責任を以下に示す。

・全職員に対してセキュリティ意識が浸透するよう啓発に努める。

・全職員が情報セキュリティの管理体制の中で役割を果たすことに対して、支援・指導を行う。

4.2　教育

情報セキュリティは、業務に携わる者全てが遵守しなければ維持・向上が難しい。情報セキュリティ規程の適用対象者に対して、入社時・定期的もしくは適宜、情報セキュリティ教育を実施していく必要がある。情報セキュリティ教育は、情報セキュリティ意識および技術的側面（システム等）の向上の両面から行う。

4.3　採用時、退職時の管理

業務に従事する者の行動が各法人・チームの情報セキュリティの脅威にならないようにするために、雇用にあたっては、情報セキュリティ規程の遵守や違反者に対する処置、機密保持について明確にした同意書を取得する。また、退職時には確認書をとり退職後の機密保持義務（機密を保持すべき期限等、内容についてはその都度定める）について確認し、また、情報資産の返却等の管理を実施する。

4.4　外部委託先などの管理

外部委託先が各法人・チームの業務に従事する場合は、当情報セキュリティ規程の準拠を条件とした業務委託契約を取り交わす。なお、先方の契約書を使用する場合、別途情報セキュリティに関する覚書を取り交わす。

派遣元の社員が各法人・チームの業務に従事する場合は、当該派遣元と各法人・チームとの間で派遣契約を取り交わすとともに、当該派遣社員と各法人・チームの間でも契約を取り交わす。

また、清掃委託先や配膳人、宅配便担当者等の各法人・チームの情報資産を直接扱うことが無い外部企業に関して、契約による情報セキュリティ確保ができない場合は、物理的なアクセスエリア制限等による管理を実施する。

第 5 章　物理的セキュリティ

5.1　セキュリティエリア

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。また、各エリアにアクセスする者を識別し、エリア毎に適切な管理を実施する。

(1)一般エリア

一般エリアとは、一般に開放しているエリアである。以下に基本的な管理要件を示す。

・全職員および第三者が自由に出入りできること。

・自由に出入り可能ではあるが、訪問者に対し受付や警備員等による牽制が行えること。

(2)オフィスエリア

オフィスエリアとは、各法人・チームの業務に従事する者が日常業務を行うエリアである。以下に基本的な管理要件を示す。

・全職員は ID カードを見える位置に所持すること。

・外部からの訪問者は職員が同行すること。

・外部からの訪問者の面談場所を定め、面談は定められた場所で行うこと。

(3)アクセス管理エリア

アクセス管理エリアとは、特に重要な情報資産を管理・運営・保管するエリアである。以下に基本的な管理要件を示す。

・オフィスエリアの管理要件を満たしていること。

・入室時のみならず、退室時にも ID カードによる開錠が必要であること。

・入退室者を特定でき、記録を残せること。

5.2　セキュリティエリアでの情報資産管理

物理的に情報資産を保護するために、情報資産の区分に応じて適切なセキュリティエリア内に設置する。また、各セキュリティエリア内での情報資産の管理要件を定める。

(1)情報資産の設置・移動

情報資産を新たに設置する場合や、他の場所から移動する場合は、情報資産の区分を考慮して、設置するセキュリティエリアを考慮すること。

(2)情報資産の廃棄

情報資産の廃棄時には、廃棄した情報資産からの情報漏洩を避けるために、情報資産の機密区分に応じて、適切な方法により廃棄すること。

(3)機器のセキュリティ

アクセス管理エリア等において重要なシステムへの電源の供給については適切な施策を実施する。また、ケーブル配線や無線 LAN 機器についても損傷や傍受等から保護する。

(4)離席時の措置

机上に重要な情報資産を放置したまま離席しないこと。また、机上のシステムについては、離席時に他者に不正操作されないようにキーボードや画面のパスワードによる保護等の適切な措置を施す。

(5)施設外における情報資産管理

施設外（自宅，電車等の公共交通機関等）で、情報資産を扱う場合は、物理的な盗難や置き忘れを避けるためにパソコン等は放置しないようにする。万が一盗難にあった場合でも、情報漏洩されない仕組みを講じる。また、重要な情報資産を持ち出す（パソコン等へデータをダウンロードする）場合は、所有者の許可を得て、各自の自己責任において管理を行う。

第 6 章　システムセキュリティ

6.1 システムの運用管理

システムおよびネットワークの運用管理においては、情報セキュリティ機能を正しく機能させるために、適切な運用管理を実施する必要がある。

(1)システム運用管理手順の整備

システムおよびネットワークについては、システム管理、システム運用、システム障害対応に関わる手順を整備する。手順書整備にあたっては、特に重要な業務においては、一人に権限が集中しないように配慮し相互牽制を図る。

(2)ユーザ管理

ユーザ識別情報(以降、ユーザ ID という)の付与、変更、削除の管理手順を定め、それに従いユーザ管理を実施する。ユーザ ID は原則として個々人に付与することとし共用は禁止する。また、定期的にユーザ ID に不要なものがないかを検査する。

(3)パスワード管理

システム毎にパスワードの付与、変更、削除の管理手順を定め、それに従いパスワード管理を実施する。また、パスワードルールを定め、システム毎にルールを実装する。更に、パスワードと同等もしくはより強固な認証技術(ワンタイムパスワード、生体認証、IC カード等)を使用する際にも、システム毎に管理手順や認証規則を定め、適切な管理や実装を行う。

(4)アクセス制御

アクセス権限の付与、変更、削除の管理手順を定め、それに従いアクセス管理を実施する。システムは、業務遂行に際して必要がある利用者だけが利用できることを原則とし、情報資産の漏洩や改ざん等の危険性を最小限にする。アクセス制御は、OS、アプリケーション、ネットワークそれぞれで実施する。アクセス権限は、必要な利用者にだけ付与し、定期的にアクセス権限の資格が妥当なものであるかを検査する。

(5)コンピュータウィルス対策

システムには、コンピュータウィルス対策機能が組み込まれたものを利用し、常時および定期的にコンピュータウィルスチェックを行うことで、コンピュータウィルス感染を防止する。コンピュータウィルス対策について防止、検知、報告、回復のそれぞれの観点からの措置を定め、コンピュータウィルス対策手順を整備し、それに従い運用管理を行うようにする。

(6)システム形態毎の管理

システムの利用形態は多種多様となってきており、情報セキュリティ機能もその利用の特性に適した運用管理が必要となる。特に外部ネットワークと接続するシステムに関しては、特別な情報セキュリティ管理が必要となる。インターネットシステムや各法人・チーム内 LAN、無線 LAN、モバイルアクセス等のシステム形態毎の運用管理手順を整備し、それに従い運用管理を行うようにする。

6.2 システム開発

不正アクセスや障害からシステムを保護するために、開発するシステムに対して、そこで扱う情報資産の区分に応じて必要な情報セキュリティ機能を組み込む必要がある。また、システム開発環境において、情報資産への侵害が起こらないように適切な情報セキュリティ対策を考慮する。

(1)システムの企画および設計

システムの開発には、情報セキュリティ確保のために暗号化やコンピュータウィルス対策、アクセス制御等のセキュリティ機能の組み込みや機器選定要件等が定められた開発標準を定めて、それに従って行う。

(2)システム形態毎の開発管理

システムの利用形態は多種多様となってきており、情報セキュリティ機能もその利用の特性に適したものを組み込む必要がある。特にインターネット等の外部ネットワークと接続するシステムに関しては、特別な情報セキュリティ対策が必要となる。インターネットシステムやモバイル環境等のシステム形態毎の開発標準を定めて、開発を行うようにする。

(3)開発環境

ソースプログラム、ライブラリおよびデータは重要な情報資産として管理し、不正利用されないように管理する。また、開発環境は本番運用環境と分離し、開発環境においては本番データをテストには利用しない。その必要が生じた場合には、本番運用環境と同様の情報セキュリティ対策を開発環境においても講じる。

6.3 システムの利用

システムに情報セキュリティ対策機能が盛り込まれていても、利用者がそれを正しく利用できなければ情報資産を保護するための情報セキュリティを確保することはできない。利用者がシステムの特性を理解し、正しく扱える必要がある。

(1)システムの利用手順の整備

情報資産の利用者が適切にシステムを利用できるように、システムの利用ガイドを整備し、それに従いシステムを利用できるようにする。利用ガイドは、各法人・チーム内のシステムやインターネット接続等のシステム形態毎に整備し、ユーザ ID およびパスワードの管理やコンピュータウィルス対策、情報資産の漏洩防止等を考慮したものとする。

(2)システムの利用範囲の限定

システムはビジネスに使用するのが第一の目的であり私的利用、業務目的外のソフトウェアの導入およびあらかじめ決められた情報セキュリティに関する設定変更を禁止する。

第 7 章 ビジネス継続管理

7.1 計画の策定

情報セキュリティ事件・事故、情報システム障害、自然災害等の影響による被害を最小限に止め、速やかに復旧、業務継続を図るために、緊急時のビジネス継続計画を策定する。

尚、ガイドラインでは「情報セキュリティ事件・事故発生時の対応」について取扱いを定める。

7.2 情報セキュリティ事件・事故発生時の対応

情報セキュリティ事件・事故が発生した場合は、情報セキュリティ事件・事故対応ガイドラインに基づき報告、対処を実施し、回復を行う。情報セキュリティ事件・事故後には、事件・事故原因を突き止め、必要に応じて計画に反映させる。

7.3 情報システム障害発生時の対応

情報システム障害が発生した場合は、定められた手順に基づき報告、対処を実施し、回復を行う。情報システム障害後には、障害原因や事故原因を突き止め、必要に応じて計画に反映させる。

7.4 自然災害等発生時の対応

自然災害等が発生した場合は、自動車リサイクル災害対策規定に基づき報告、対処を実施し、復旧を行う。また、策定されたビジネス継続計画が正しく機能するか否かを定期的な訓練により検証するとともに評価を実施し、必要に応じて計画の更新を行う。

第 8 章　規程の遵守

8.1 法律の遵守

(1)関連法規の遵守

全職員は、情報セキュリティに関するすべての法規および契約上の要求事項を遵守し、これに従わなければならない。

(2)著作権の遵守

全職員は、ソフトウェア製品をはじめとする情報の利用ライセンスを正しく取得し、著作権を守る。

情報セキュリティ管理者はソフトウェア製品、書籍、および印刷物をはじめとする情報の著作権を守るために指導、監督する。

8.2 自己点検及び監査

(1)自己点検の実施

情報セキュリティ規程に沿った情報セキュリティ対策が実施されているか否かについて、各法人・チームの情報セキュリティ管理者は、自己点検を行わなければならない。

自己点検は自己点検シートなどを使用し、適宜実施する。

情報セキュリティ部会は、各法人・チームの自己点検結果をとりまとめ、情報セキュリティ規程の更新の際に参照する情報として活用することとする。

(2)情報セキュリティ監査の実施

情報セキュリティ監査は、情報システム監査の一環として、適宜実施する。

また監査人の独立性保持の観点から必要に応じて、情報セキュリティ監査を業とする外部コンサルタント、監査法人等による監査を検討する。

8.3 罰則

(1)就業規則(雇用契約)による措置

情報セキュリティに関する違反に対する対応について就業規則に基づく措置を受けることとなる。

(2)情報セキュリティ規程を遵守できない場合の措置

やむを得ない事情、事態により情報セキュリティ規程を遵守できない場合、情報セキュリティ責任者の判断を得て適切に対処する。この場合、情報セキュリティ管理者はリスクを最小化するような代替措置、今後のアクションプランの立案等を実施する。