Ver.1

ADEC 消去プロセス認証ガイド

ADEC – データ適正消去実行証明協議会

目次

目的

本ガイドは、データ消去業務に携わる事業者の業務プロセスにおいて留意すべき脅威（リスク）とそれを低減するための管理策を提示しています。

これにより、安全・安心な消去業務管理手順構築の一助となること、ADEC 消去プロセス認証取得のガイドとしてご利用いただくことを目指しております。

適用範囲

データ消去プロセスの適用範囲は、業務プロセス中、次の局面とします。

・対象媒体の入庫

・対象媒体の保管

・対象媒体のデータ消去

・消去証明書の発行

※データ消去をおこなう拠点における、入庫から証明書発行までのプロセス

ISMS（ISO/IEC 27001）の参照

データ消去業務において、情報セキュリティ対策の導入は必須となります。そのため、世界標準である ISO/IEC 27001 の管理策を参照する形で、本ガイドは作成されております。

本文中に登場する A.〇.〇 （〇は数字）は、すべて ISO/IEC 27001 附属書 A に列記された各管理策の項番と紐ついております。

さらに詳しい安全管理策の策定を検討する場合は、 ISO/IEC 27001 及び ISO/IEC 27002 の各項番を参照してください。

求められる管理策

データ消去プロセスにおいては、次の局面における脅威に対する管理策を検討する必要があります。ADEC 消去プロセス認証審査においても文書化された管理策およびエビデンス（証跡）の提示を求めることとなります。

機器（媒体）への脅威

消去対象となる機器に搭載されている記憶媒体のデータ消去を確実にするため、当該記憶媒体への脅威に対する管理策の導入および運用状況を評価する。

機器（媒体）の盗難

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☐証明書発行

A.8.1.1 資産目録

管理目的：情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

【望まれる管理策】

消去対象機器（媒体）の盗難や紛失のリスクを低減するため、対象機器（媒体）の管理が要求される。機器には複数台の記憶媒体が搭載されている場合があるため、機器単位での管理では不十分である。適時、機器に搭載された記憶媒体を確認し、記憶媒体ごとに管理しなければならない。

また、盗難等を行う者により、管理情報が改ざんされ対象機器（媒体）の記録が消去される恐れを予防する措置も必要である。

実施状況の確認
①入庫時の機器（媒体）を記録する ②消去後の機器（媒体）を記録する ③記録は、機器に搭載されたすべての媒体を識別できる方法を用いる ④記録は、不正の発見を妨げることのない期間、保管されている*01 ⑤記録の管理において漏えい、改ざん、滅失に対する予防策を講じている*02
証跡例（更新/確認頻度）
消去媒体管理台帳（都度）

*01：依頼者が ISMS（１年ごと）、PMS（２年ごと）の審査を受審することを考慮し、２年以上３年以下の保管期間が望ましい。

*02：記録がどのような手段で管理されているかにより記録の信頼性は異なる。

「Excel 等電子ファイルによる管理」は、データの改ざんが容易であるため、ファイルへのアクセス権の設定、更新履歴の記録、アクセス者の記録、定期的な確認、バックアップ等により改ざんを防止しなければならない。

「手書きによる管理」は、容易に消去できないインクで記されたものであれば、改定箇所がわかりやすいため、改ざんは容易ではない。しかし、大量の件数をこなさなければならない場合、記録がずさんになりやすい。

「専用システムによる管理」は、もっとも確実な管理策であるが、操作者が特定できない仕組み、たとえば、複数の人員が同一 ID を利用することは避けなければならない。このようなシステムの利用は、手入力の際の誤入力の予防措置も考えなければならない。たとえば、バーコード等を利用した対象機器（媒体）の特定等が可能な仕組みが導入されている場合は、信頼性が高くなる。

A.8.1.2 資産の管理責任

管理目的：目録の中で維持される資産は、管理されることが望ましい。

【望まれる管理策】

消去対象機器（媒体）は、消去が完了するまで、さまざまな脅威＝リスクから守らなければならない。組織は、そういった「リスク」に対する責任を負う者を決定しなければならない。責任者は、作業現場における監督者であることが望ましい。

実施状況の確認
①A.8.1.1 の記録には、機器（媒体）の管理責任者を決定し、記録する
証跡例（更新/確認頻度）
消去媒体管理台帳（都度）

A.8.2.2 情報のラベル付け

管理目的：情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。

【望まれる管理策】

入庫時に記録された機器（媒体）に対して、管理コード（ID）を付与し、ラベル等を張り付けることにより、所在確認や進捗管理が容易になる。ラベルは「個体の識別」のために用いるのが一般的だが、さらに、処理ステータスを識別できるような措置をとっている場合、評価が高くなる。

実施状況の確認
① 機器（媒体）は、ラベル付け（ID づけ）もしくはそれに代わる管理方法により、目視で識別可能な状態である
証跡例（更新/確認頻度）
機器（媒体）へのラベル付け（ID づけ） ・ラベル付けにより、個体を識別できる ・ラベル付けにより、処理ステータス（処理前、処理中、処理後等）を識別できる

機器（媒体）に格納されている情報の盗難（不正コピー）

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☐証明書発行

A.8.3.3　物理的媒体の輸送

管理目的：情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護することが望ましい。

【望まれる管理策】

入庫から保管庫への移送時、保管庫から消去作業場への移送時に消去対象機器（媒体）に格納された電子データが複製されることを予防しなければならない。

実施状況の確認
①移送時の手順の明文化 ②監視体制の導入（監視カメラ、複数人の相互監視等）
証跡例（更新/確認頻度）
消去業務手順書（手順変更前） 消去業務担当者名簿（都度） フロアレイアウト図（レイアウト図は、レイアウト変更前に見直しが行われていることが望ましい）※審査では、最新版を確認する。 消去業務実施記録・移送記録（都度） 監視カメラ映像（任意）※審査では、作業プロセスを参照し、妥当と思われる期間、映像が保管されているかどうかを確認する。

再利用または廃棄した機器（媒体）を復元する試み

【対象プロセス】

□入庫　□保管庫へ移送　□保管　□作業区域へ移送　☒消去　☒証明書発行

A.12.4.3 実務管理者及び運用担当者の作業ログ

管理目的：システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューすることが望ましい。

【望まれる管理策】

消去済機器（媒体）からデータを復元する試みは業務ルールの中で禁止しなければならない。しかし、故意に消去を失敗させ、正常終了した記録を残し、その後、復元を試みることは不可能ではない。そのため、消去が正常に終了したことを証明するためのログの保管が必要である。また、ログは、プログラム自体が生成するものが望ましい。※消去プログラムはフリーウェア等は禁止、

実施状況の確認
①消去プログラムが生成する作業ログの確認 ②消去プログラムが生成する作業ログの保管 ③異常終了時の対応手順の明文化 ④作業ログの捏造、改ざんを防止するための管理策
証跡例（更新/確認頻度）
消去業務手順書（手順変更前）※復元の試みを禁止していること 消去プログラムが生成する作業ログ（該当機器（媒体）出庫確認後、妥当と思われる期間の保管）

顧客情報の漏えい

【対象プロセス】

☒入庫　☐保管庫へ移送　☐保管　☐作業区域へ移送　☐消去　☒証明書発行

A.12.2.1 マルウェアに対する管理策

管理目的：マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施することが望ましい。

【望まれる管理策】

消去対象機器（媒体）の管理データに顧客情報が含まれる場合がある。当該管理データを格納する PC がウィルスに感染し、外部に当該管理データが流出する脅威に対する措置を講じる必要がある。

実施状況の確認
①業務用 PC においては許可されていないソフトウェアの使用を禁止する ②ウィルス対策ソフトを導入する ③ネットワークを分離する（外部からの侵入を予防する）
証跡例（更新/確認頻度）
許可済みソフトウェアリスト（毎年） ※情報セキュリティルールブック（ソフトウェアのインストールを規定しているもの） ウィルス対策ソフト（定期更新） ネットワーク図（システム変更前） ウィルス感染時対応手順書（適時）

A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護

管理目的：プライバシー及び PII の保護は、関連する法令及び規制が適用される場合には、その要求に従って確実にすることが望ましい。

【望まれる管理策】

顧客情報は受注管理、請求書の発行等の業務においては必要であるが、消去業務においては不要である。顧客情報と消去対象機器（媒体）が紐ついていることにより、作業者が記憶媒体に格納されている電子データに興味をもち、悪意のある作業者による不正コピーのリスクが高まる恐れがある。顧客情報はできるだけ秘匿化されている必要がある。

実施状況の確認
①作業指示書等へは顧客名を明示しない
証跡例（更新/確認頻度）
作業指示書（都度）

A.12.6.1 技術的ぜい弱性の管理

管理目的：利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得することが望ましい。また、そのようなぜい弱性に組織がさらされている状況を評価することが望ましい。さらに、それらと関連するリスクに対処するために、適切な手段をとることが望ましい。

【望まれる管理策】

消去対象機器（媒体）の管理データに顧客情報が含まれる場合がある。当該管理データを格納する PC にインストールされた OS やソフトウェアの設定やぜい弱性対策が不十分であると、外部に当該管理データが流出する恐れが高まるため、ぜい弱性への対応措置を講じる必要がある。

実施状況の確認
①業務用 PC の設定条件の明文化 ②ぜい弱性対策基準の明文化 ③OS のアップデート手順の明文化

証跡例（更新/確認頻度）
業務用 PC 設定基準書 ぜい弱性対策基準書 OS アップデート手順書 OS/ソフトウェアアップデート記録

技術的障害

消去結果の信頼性を確実にするため、消去プログラム、消去専用機器に対する管理策の導入状況を評価する。

消去用機器・ソフトウェアの故障による不完全な消去

【対象プロセス】

□入庫　□保管庫へ移送　□保管　□作業区域へ移送　☒消去　□証明書発行

A.8.1.1 資産目録

管理目的：情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

【望まれる管理策】

消去プログラム、消去専用機器を紛失や故障から守るため、また、利用を許可されないプログラムが紛れ込むのを防ぐため、消去プログラム、消去専用機器を特定し、管理しなければならない。

実施状況の確認
①消去用機器・ソフトウェアの管理台帳 ②記録は、不正の発見を妨げることのない期間、保管されていること"

証跡例（更新/確認頻度）
消去用機器・ソフトウェア管理台帳（都度）

A.8.1.2 資産の管理責任

管理目的：目録の中で維持される資産は、管理されることが望ましい。

【望まれる管理策】

消去プログラム、消去専用機器は、さまざまな脅威＝リスクから守らなければならない。組織は、そういった「リスク」に対する責任を負う者を決定しなければならない。責任者は、作業現場における監督者であることが望ましい。

実施状況の確認
①A.8.1.1 の記録には、消去プログラム、消去専用機器の管理責任者を決定し、記録する
証跡例（更新/確認頻度）
消去用機器・ソフトウェア管理台帳（都度）

A.8.2.2 情報のラベル付け

管理目的：情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。

【望まれる管理策】

消去プログラムが格納された媒体、消去専用機器に対して、管理コードを付与し、ラベル等を張り付けることにより、所在確認が容易になる。

実施状況の確認
①機器（媒体）は、ラベル付けもしくはそれに代わる管理方法により、目視で識別可能な状態である

証跡例（更新/確認頻度）
ラベル付けされた媒体、機器（都度）

消去用機器・ソフトウェアの誤作動による不完全な消去

【対象プロセス】

□入庫　□保管庫へ移送　□保管　□作業区域へ移送　☒消去　□証明書発行

A.15.2.2　　供給者のサービス提供の変更に対する管理

管理目的：関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理することが望ましい。

【望まれる管理策】

ソフトウェア提供者とは利用契約書等で各社の責任やバージョンアップ等について明確にし、消去ソフトウェアの信頼性を維持しなければならない。

実施状況の確認
①消去用機器・ソフトウェアの提供者と次の事項について取り決めをする 1）不具合等の修正に関する取り決め 2）バージョンアップ版の提供に関する取り決め 3）稼働環境（OS 等）の変更に関する取り決め 4）サポート期間に関する取り決め
証跡例（更新/確認頻度）
ソフトウェア利用契約書（適時）

許可されない行為

第三者の侵入、不正なソフトウェアの利用等、許可されない行為を監視し、予防するための物理的な安全管理策を中心に導入状況を評価する。

許可されない第三者の侵入によるインシデント

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☐証明書発行

A.11.1.1 物理的セキュリティ境界

管理目的：取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いることが望ましい。

【望まれる管理策】

作業区域は、他の区域と物理的境界を設け、許可されない第三者の侵入を防がなければならない。

実施状況の確認
①作業区域は他の区域と物理的境界を設ける
証跡例（更新/確認頻度）
フロアレイアウト図（レイアウト変更前） 消去業務担当者名簿（都度）

A.11.1.2 物理的入退管理策

管理目的：セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護することが望ましい。

【望まれる管理策】

作業区域への要員の入退室を管理し、許可されない第三者の侵入を防がなければならない。

実施状況の確認
①作業区域への許可されない第三者の侵入を防止する策を講じる ②作業区域への入退室を記録する ③作業者を識別する
証跡例（更新/確認頻度）
フロアレイアウト図（レイアウト変更前） 入退室記録（都度） カードキー付与情報（毎月/都度） 個人識別カード、ネームプレート等

許可されない機器・ソフトウェアの使用

【対象プロセス】

☐入庫　☐保管庫へ移送　☐保管　☐作業区域へ移送　☒消去　☐証明書発行

A.11.1.5 セキュリティを保つべき領域での作業

管理目的：セキュリティを保つべき領域での作業に関する手順を設計し、適用することが望ましい。

【望まれる管理策】

要員が作業区域へ持ち込み可能なものを限定することで、不正なデータの持ち出し等を防がなければならない。

実施状況の確認

①許可されていない機器（ソフトウェア含む）の作業区域への持ち込みを禁止する ②作業着を着用させる場合は、機器を忍ばせ易いポケット等のないものを採用する
証跡例（更新/確認頻度）
許可されていない機器（ソフトウェア含む）の持ち込みを禁止する文書（適時） 作業着、私物持ち込み用バッグ等 金属探知機

許可されない区域・環境での作業

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☐証明書発行

A.8.1.3 資産利用の許容範囲

管理目的：情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施することが望ましい。

【望まれる管理策】

消去対象機器（媒体）の保管、処理区域、作業者等を明確にすることにより、許可されない不正な取扱いを防がなければならない。

実施状況の確認
①機器（媒体）の保管区域、処理区域の明文化 ②機器（媒体）の移送手順の明文化 ③機器（媒体）へのアクセス権の明文化 ④上記ルールの実施記録と定期的な評価
証跡例（更新/確認頻度）
消去業務手順書（手順変更前）

消去業務担当者名簿（都度）
フロアレイアウト図（レイアウト変更前）
消去業務実施記録（都度）

A.11.2.5 資産の移動

管理目的：装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さないことが望ましい。

【望まれる管理策】

消去対象機器（媒体）の保管、処理区域を明確にし、適時監督することにより、許可されない不正な持出を防がなければならない。

実施状況の確認
①機器（媒体）の所在確認 ②監視体制の導入（監視カメラ、複数人の相互監視等） ③退室時のチェック体制　*3
証跡例（更新/確認頻度）
消去媒体管理台帳（都度）※サンプリングで媒体の個体確認をおこなう 監視カメラ（任意）映像（該当機器（媒体）出庫確認後、妥当と思われる期間の保管） 金属探知機、身体検査、手荷物検査、等

*3：次のような脅威に対する対策が必要である。

・消去対象機器（媒体）の持ち出し：機器または機器から取り外した記憶媒体等を鞄に入れて持ち出す場合がある。また、窓から屋外に放り投げ、あとから回収する場合がある。

・消去対象機器（媒体）に記憶されたデータの持ち出し：USB メモリ、SD カード、CD-ROM、DVD-ROM 等の記憶媒体にデータを複製し、その媒体を持ち出す場合がある。また、窓から屋外に放り投げ、あとから回収する場合がある。

委託先、派遣社員による脅威

委託先、派遣社員による不正な行為を監視し、予防するための監督体制の導入状況を評価する。ここでいう委託先とは、作業区域内における作業を委託しているケースを意味し、消去対象機器（媒体）を他所に移送して消去業務をおこなうことではない。

監督不行き届き

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☐証明書発行

A.15.1.2 供給者との合意におけるセキュリティの取扱い

管理目的：関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意することが望ましい。

【望まれる管理策】

委託先、派遣社員は事前に評価し、責任の範囲を明文化しなければならない。また、従業者と同等の情報セキュリティに関する力量を身につけさせなければならない。

実施状況の確認
①委託先は契約前に評価する ②情報セキュリティに関する条項を含む契約書の締結 ③委託先の作業者の監督 ④情報セキュリティ教育の実施（少なくとも 1 回/年）
証跡例（更新/確認頻度）
委託先評価記録（毎年） 業務委託契約書 消去業務担当者名簿（都度）

情報セキュリティ教育記録（都度）

その他の脅威

その他、起こり得る脅威に対する安全管理策に関する導入状況を評価する。

消去用機器・ソフトウェアの操作ミスによる不完全な消去

【対象プロセス】

□入庫　□保管庫へ移送　□保管　□作業区域へ移送　☒消去　□証明書発行

A.12.1.1 操作手順書

管理目的：操作手順は、文書化し、必要とする全ての利用者に対して利用可能とすることが望ましい。

【望まれる管理策】

操作ミスによる不完全な消去を防ぐため、消去用機器・ソフトウェアの操作手順に関する文書を準備し、消去業務にあたる者に手順通りの操作ができるよう訓練させなければならない。また、作業工程で不完全な消去等の不適合が発生した場合の対応についても、手順に関する文書に含めなければならない。

実施状況の確認
①作業手順の明文化 ②作業手順の訓練
証跡例（更新/確認頻度）
消去業務手順書（手順変更前） 消去業務における適合/不適合の基準 訓練実施記録（都度）

職権の乱用

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☒証明書発行

A.6.1.2　職務の分離

管理目的：相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離することが望ましい。

【望まれる管理策】

あらゆる業務は、過失や悪意を持った行為を予防するため、作業者と監督者は異なる人員でなければならない。

実施状況の確認
①情報セキュリティ責任者、作業管理者、作業者等の役割の明文化 ②指示と報告の記録
証跡例（更新/確認頻度）
組織体制図（体制変更前） 消去業務実施記録（都度）

作業者の力量不足によるインシデント

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☒証明書発行

A.7.1.1 選考

管理目的：全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行うことが望ましい。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行うことが望ましい。

【望まれる管理策】

当該業務にあたる人員は、業務を任せるに足る力量を有しているか、採用選考時に評価しなければない。

実施状況の確認
① 雇用にあたっては、本人確認および経歴確認を行う ② 就業規則に罰則を明記する
証跡例（更新/確認頻度）
就業規則（適時） 採用基準とプロセスを確認（本人確認）

A.7.1.2 雇用条件

管理目的：従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載することが望ましい。

【望まれる管理策】

当該業務にあたる人員に対しては、規則に従わなかった場合の懲罰について、採用時に本人に認識させなければならない。

実施状況の確認
①雇用契約書を締結する ②雇用終了後も有効である機密保持契約を締結する
証跡例（更新/確認頻度）

雇用契約書（適時）
機密保持契約書（適時）

A.7.2.2 情報セキュリティの意識向上、教育及び訓練

管理目的：組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受けることが望ましい。

【望まれる管理策】

当該業務にあたる人員は、情報セキュリティインシデントの防止を目的とした教育を受けなければならない。教育には、①機密保持に関する規定、②規定に従わなかった場合に与えられる罰則、を含めなければならない。

実施状況の確認
① 情報セキュリティ教育の実施（少なくとも 1 回/年）と力量評価 ② 要員に求める力量の明文化 ③ 本人のセキュリティ意識の確認方法（リテラシーと能力の 2 面から確認）
証跡例（更新/確認頻度）
消去業務を実施するうえで必要とされる力量の定義と、要員の力量評価記録 情報セキュリティ教育教材（適時） 情報セキュリティ教育実施記録（都度） 理解度確認記録（都度） スキルマップ（例）

不十分なインシデント対応

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☒証明書発行

A.16.1.1 責任及び手順

管理目的：情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立することが望ましい。

【望まれる管理策】

情報セキュリティ事象が発生した際、被害の拡大を最小限にするため、あらかじめ対応手順が確立されていることが望ましい。さらに、情報セキュリティにおける事業継続計画が策定され、訓練が実施されることが推奨される。

実施状況の確認
a)組織において、次の手順が策定され、十分に伝達されることを確実にするために、管理層の責任を確立する。 1)インシデント対応の計画及び準備のための手順 2)情報セキュリティ事象及び情報セキュリティインシデントを監視、検知、分析及び報告するための手順 3)インシデント管理活動のログを取得するための手順 4)法的証拠を扱うための手順 5)情報セキュリティ事象の評価及び決定のための手順、並びに情報セキュリティ弱点の評価のための手順 6)対応手順（段階的取扱い、インシデントからの回復の管理、並びに内部及び外部の要員又は組織への伝達のための手順を含む。） b)確立する手順では、次の事項を確実にする。 1)組織内の情報セキュリティインシデントに関連する事項は、力量のある要員が取り扱う。 2)セキュリティインシデントを検知及び報告する場合の連絡先を定める。 3)情報セキュリティインシデントに関連した事項を取り扱う関係当局、外部の利益団体又は会議との適切な連絡を保つ。

c)報告手順には、次の事項を含める。 1)情報セキュリティ事象が発生した場合に、報告作業を助け、報告する者が必要な全ての処置を忘れないよう手助けするための情報セキュリティ事象の報告書式の作成 2)情報セキュリティ事象が発生した場合にとる手順。例えば、詳細全て（不順守又は違反の形態、生じた誤動作、画面上の表示など）の記録を直ちにとる、直ちに連絡先に報告し、協調した処置だけをとる。 3)セキュリティ違反を犯した従業員を処罰するために確立された正式な懲戒手続への言及 4)情報セキュリティ事象の報告者に、その件の処理が終結した後で結果を知らせることを確実にするための適切なフィードバックの手続 d）情報セキュリティにおける事業継続計画書の有無を確認する 1）広域災害等における消去対象機器（媒体）の安全確保 2）事業継続計画発動基準
証跡例（更新/確認頻度）
情報セキュリティインシデント対応手順書（適時） 情報セキュリティインシデント管理票（都度） 事業継続計画および訓練の記録（消去対象機器（媒体）の保護、記録の保持、などが含まれていること）

契約違反

【対象プロセス】

□入庫　□保管庫へ移送　□保管　□作業区域へ移送　☒消去　☒証明書発行

A.18.1.1適用法令及び契約上の要求事項の特定

管理目的：各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つことが望ましい。

【望まれる管理策】

リユース機器については、リカバリ領域/区域を消去することができないため、当該領域にデータを格納している場合、そのデータが残る恐れがある。リユース処理を行う事業者は、依頼者に文書で説明し、依頼者の判断・同意を得る必要がある。

実施状況の確認
①リユース機器に対する考慮：リユース目的のためリカバリ領域/区域を消去対象外とすることのリスクを説明し、依頼者の同意を得る ②作業の結果が契約通りであることを確認する
証跡例（更新/確認頻度）
作業指示書（適時） □リユースに対する依頼者の同意 □リユース機器：消去領域/区域の結果確認 □消去業務実施記録

権限の詐称

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☒証明書発行

A.9.2.1 利用者登録及び登録削除

管理目的：アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施することが望ましい。

【望まれる管理策】

作業区域、消去用機器、ソフトウェア等へのアクセス権を明確にし、管理しなければならない。

実施状況の確認
管理システムを利用する場合 ①利用者 ID は利用者ごとに異なるものでなければならない ②利用者は、自らに付与された利用者 ID を他者に貸与してはならない ③やむをえず共有 ID を発行する場合、利用者 ID を貸与する場合は、管理責任者の承認を必須とする 目視による監督を行う場合 ①利用者へのアクセス権付与状況は明文化する。
証跡例（更新/確認頻度）
管理システムを利用する場合 ・システムのアカウント情報（毎月/都度） ・カードキー付与情報（毎月/都度） 目視による監督を行う場合 ・消去業務担当者名簿（都度）

A.9.2.5 利用者アクセス権のレビュー

管理目的：資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューすることが望ましい。

【望まれる管理策】

作業区域、消去用機器、ソフトウェア等へのアクセス権が、正しく付与されているか、定期的に確認しなければならない。

実施状況の確認
管理システムを利用する場合 ①利用者のアクセス権を見直す頻度を決定する 目視による監督を行う場合

①作業区域への入退室を記録する ②入退室記録は管理者が定期的に評価する
証跡例（更新/確認頻度）
管理システムを利用する場合 ・システムのアカウント情報（毎月/都度） ・カードキー付与情報（毎月/都度） ・各システムログ（毎月/都度） 目視による監督を行う場合 ・入退室記録（都度）

A.9.2.6 アクセス権の削除又は修正

管理目的：全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正することが望ましい。

【望まれる管理策】

人事異動、役割の変更等が発生した場合は、すみやかに当人のアクセス権を見直す必要がある。

実施状況の確認
管理システムを利用する場合/目視による監督を行う場合 ①利用者 ID を持つものが、その業務を離れる場合を想定し、そのアクセス権の停止・消去の時期を決定する。
証跡例（更新/確認頻度）
管理システムを利用する場合 ・システムのアカウント情報（毎月/都度） ・カードキー付与情報（毎月/都度） ・各システムログ（毎月/都度）

目視による監督を行う場合 ・消去業務担当者名簿（都度）

不十分なレビュー

【対象プロセス】

☒入庫　☒保管庫へ移送　☒保管　☒作業区域へ移送　☒消去　☒証明書発行

A.18.2.1 情報セキュリティの独立したレビュー

管理目的：情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施することが望ましい。

【望まれる管理策】

定められた手順、安全管理策が実施され、運用されることを確実にするため、あらかじめ定めた間隔で自己点検を実施することが望ましい。第一者監査（内部監査）を実施している場合は、さらに信頼性を高めることになる。

実施状況の確認
①　内部監査は、あらかじめ計画をたて、それに従い実施する。 ②　監査員は、力量を有する、中立的立場の人員を任命する。 ③　不順守がある場合は、原因を特定し、適切な是正処置を実施する。 ④　点検が形骸化していないこと
証跡例（更新/確認頻度）
自己点検の記録 ・少なくとも 1 回/月実施していること ・点検を行う者はマネジメントまたは中立的な立場であること 内部監査を実施している場合は、高く評価する。

・内部監査計画書（適時）
・内部監査の記録（適時）※項目を確認する？
・内部監査報告書（適時）
・内部監査員の力量を評価する記録（適時）※作業者ではなく監督者であること
是正処置の記録（適時）*4

*4：是正処置には、次の項目を含める

・不適合の原因分析（失念、注意力欠如、ヒューマンエラー等は原因分析にはならない。なぜ失念したか、なぜ注意力が欠如したのか、なぜヒューマンエラーが発生したか等、根本的な原因を特定しなければならない。）

・原因の除去（教育、指導、訓告等、精神に訴えるものは有効とはいえない。

・是正処置のレビュー（是正処置が原因除去に有益であったか否かについて、適切なタイミングで評価しなければならない。）

ADEC 消去証明書発行

ADEC 消去証明書を発行するためには、ADEC 認証を取得した消去ソフトおよび作業環境を構築しなければならない。

ADEC 環境の構築

【対象プロセス】

☐入庫　☐保管庫へ移送　☐保管　☐作業区域へ移送　☒消去　☒証明書発行

ADEC 環境の構築

実施状況の確認
① ID/パスワードによるログイン認証をおこなう ② 利用者ごとに異なるな ID/パスワードを発行する ③ ADEC 情報セキュリティポリシーに準じた作業環境を構築する
証跡例（更新/確認頻度）
① ID/パスワードによる認証を行われていることを確認 ② 利用者ごとに異なる ID が発行されていることを確認 ③ 消去ソフトウェアベンダーが発行する「環境構築マニュアル」通りに環境が構築されていることを確認

認証の取得

ISMS、プライバシーマーク、品質マネジメント等を取得している事業者は、マネジメントシステムが構築されていると認められる。

情報セキュリティ等の認証

情報セキュリティ認証等

実施状況の確認
ISMS（ISO/IEC27001）、プライバシーマーク（JIS Q 15001）、品質マネジメント（ISO 9001）、またはその他の認証
証跡例（更新/確認頻度）
認証番号を確認する

更新履歴

2020/10/05　　ドラフト版　発行

発行元

データ適正消去実行証明協議会（ADEC）

〒107-0052 東京都港区赤坂 1-3-6

赤坂グレースビル

℡ 03-3560 -8440

https://adec-cert.jp/