鉄道分野における情報セキュリティ確保に係る安全ガイドライン

第3版

平成28年4月1日　改訂

国　土　交　通　省

＜目次＞

1. 「安全ガイドライン」策定の背景

1.1 「安全ガイドライン」策定までの経緯

1.1.1 重要インフラの情報セキュリティ対策に係る行動計画

重要インフラに係る行動計画は、重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画であり、2005 年（平成 17 年）に情報セキュリティ政策会議が提示した、IT障害から重要インフラを防護し、重要インフラ事業者等の事業継続性を確保するために取るべき対策についての基本的方向性を踏まえ、同年に「重要インフラの情報セキュリティ対策に係る行動計画」（以下「第1次行動計画」という。）が決定された。

さらに、第1次行動計画において構築された重要インフラの基本的な情報セキュリティ対策や官民の情報共有の枠組みを基礎とし、国として取り組むべき施策を示した「重要インフラの情報セキュリティ対策に係る第2次行動計画」（以下「第2次行動計画」という。）が 2009 年（平成 21 年）に決定された。第2次行動計画では、刻々と変化する社会環境や技術環境に的確に対応するため、新たに「環境変化への対応」についての施策が追加された。

「重要インフラの情報セキュリティ対策に係る第3次行動計画」（以下「第3次行動計画」という。）が 2014 年（平成 26 年）5月 25 日に決定され、「サイバーセキュリティ戦略（2013 年（平成 25 年）6月情報セキュリティ政策会議決定）」を踏まえつつ、第2次行動計画における施策群の評価によって得られた良好事例、要改善事例等の知見が反映されるとともに、東日本大震災発災時のシステム障害、データ滅失等への対応において得られた知見等の活用に加え、刻々と変化する社会環境・技術環境、近年の複雑化・巧妙化するサイバー攻撃の趨勢への適切な対応が反映された。

1.1.2 重要インフラにおける情報セキュリティ確保に係る「安全基準等」

第3次行動計画は、次の5つの施策から構成されている。

- ◆ 安全基準等の整備及び浸透
- ◆ 情報共有体制の強化
- ◆ 障害対応体制の強化
- ◆ リスクマネジメント
- ◆ 防護基盤の強化

このうちの第一項にある「安全基準等」については、平成 27 年 5 月 25 日にサイバーセキュリティ戦略本部において決定された「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第4版）」（以下「指針」という。）において、位置づけや規定が望まれる項目等が述べられている。

本「安全ガイドライン」は、国土交通省の所管する鉄道分野の「安全基準等」として、「指針」に基づいて策定するものである。

1.1.3 国土交通省における取り組み

国土交通省では、「行動計画」及び「指針」に則り、所管する3分野（鉄道、航空、物流）における各事業分野、及び関連事業者の情報セキュリティ対策の現状に配慮しながら、各事業分野における情報セキュリティ対策の向上に資する望ましい情報セキュリティ対策の水準をまとめるため、「重要インフラ情報セキュリティ対策検討ワーキンググループ」を開催し、「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」の初版を策定した。（初版策定時のワーキンググループメンバーについては、下表参照）

以降、指針の改正や世の中の情勢を踏まえ、適宜本ガイドラインを改訂している。

重要インフラ情報セキュリティ対策検討 WG 鉄道検討分科会構成メンバー

	会　　社　　名
鉄道事業者 （○印会社は幹事会社）	北海道旅客鉄道株式会社 ○ 東日本旅客鉄道株式会社 ○ 東海旅客鉄道株式会社 西日本旅客鉄道株式会社 四国旅客鉄道株式会社 九州旅客鉄道株式会社 東武鉄道株式会社 西武鉄道株式会社 京成電鉄株式会社 京王電鉄株式会社 小田急電鉄株式会社 東京急行電鉄株式会社 ○ 京浜急行電鉄株式会社 ○ 東京地下鉄株式会社 相模鉄道株式会社 名古屋鉄道株式会社 近畿日本鉄道株式会社 南海電気鉄道株式会社 ○ 京阪電気鉄道株式会社 阪急電鉄株式会社 阪神電気鉄道株式会社 西日本鉄道株式会社 国土交通省総合政策局情報政策課

	国土交通省鉄道局 社団法人日本民営鉄道協会

※会社名は初版策定当時の名称です。

1.2 「安全ガイドライン」の目的と位置づけ

1.2.1 「安全ガイドライン」の目的

国民生活や社会経済活動の基盤である重要インフラにおける IT 化の進展や相互の依存関係が増大していることに伴って、各事業分野においてIT障害に対する情報セキュリティ対策を適切に行うことが、大きな課題となっている。しかしながら、情報セキュリティに関しては、対策の効果が目に見えにくいものであるため、各事業分野においては、対策が十分であるか、事業者自らが十分な対策をなしているのか、を自己検証しつつ、国民生活や社会経済活動に重大な影響を及ぼさないようIT障害から重要インフラを防御する対策を進めることが必要になる。

このため、それぞれの事業分野において、その特性に応じた必要又は望ましい情報セキュリティの水準を明示し、個々の事業者が、重要インフラの担い手としての意識に基づいて自主的な取り組みにおける努力や検証をするための目標を定めることが「安全ガイドライン」の目的である。

1.2.2 鉄道分野における「安全ガイドライン」の形態

「指針」では、「安全基準等」の形態として、以下の4つの例があることが述べられている。

① 業法に基づき国が定める「強制基準」
② 業法に準じて国が定める「推奨基準」及び「ガイドライン」
③ 業法や重要インフラ利用者からの期待に応えるべく事業者団体等が定める業界横断的な「業界標準」及び「ガイドライン」
④ 業法や重要インフラ利用者及び契約者等からの期待に応えるべく事業者自らが定める「内規」

本ガイドラインは、国が定める「ガイドライン」として策定するものであり、事業分野の特性に鑑み、事業者等が自らの情報セキュリティ対策を実施する際に参考資料として活用することを想定している。

1.2.3 「安全ガイドライン」の位置づけ

「安全ガイドライン」には、重要インフラ分野においてサービス提供継続及び重要インフラ利用者の信頼性に応えるとの観点から、サイバーテロ対策を初めとして、災害や非意図的要因などサービス提供に影響を及ぼす可能性のある様々な事象を念頭に置き、情報セキュリティ対策を実施する場合に何らかの対処がなされていることが望ましい項目、及び対処すべき内容を列挙する。また、それぞれの事業分野の特性に応じて事業者等が活用し易い基準等とするとの視点から、各事業分野の特性や現状をもとにした、想定事象、対処方針等について記述する。

このため、「安全ガイドライン」は、「指針」において求められる内容に加え、「政府機関の情報セキュ

リティ対策のための統一基準群」を初め国内外で用いられるベストプラクティスやスタンダード（基準）等をもとにした検討内容をもって構成する。

1.2.4 鉄道分野における対策項目の構成

「安全ガイドライン」における対策項目は、「指針」に述べられているPDCAサイクルに沿って、以下のガイドライン等を参考に検討し鉄道分野の状況に応じて構成する。

（1）政府機関の情報セキュリティ対策のための統一基準群

政府機関全体の情報セキュリティ対策を強化・拡充するために、「政府機関全体の情報セキュリティ対策の強化に関する基本方針（平成17年9月15日付情報セキュリティ政策会議決定）に基づき、政府機関が行うべき情報セキュリティ対策の統一的な枠組みを構築し、各省庁の情報セキュリティ水準の斉一的な引き上げを図る目的で、各府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたものである。

平成17年12月13日に全体版初版が情報セキュリティ政策会議決定されており、現在、平成26年5月19日に平成26年度版が情報セキュリティ政策会議決定されている。

（2）情報セキュリティ管理基準

組織体が効果的な情報セキュリティマネジメント体制を構築し、適切なコントロールを整備、運用するための実践規範であり、情報セキュリティ監査において、評価判定基準として用いられる。情報セキュリティに係るマネジメントサイクル確立のための標準規格であるJIS Q27001:2006附属書A、JIS Q27002:2006をもとにしている。

（3）事業継続ガイドライン

内閣府の取り組みとしての事業継続計画（BCP）の普及、促進のため、中央防災会議「民間と市場の力を活かした防災力向上に関する専門委員会」の下に設置された、「企業評価・業務継続計画ワーキンググループ」において作成されたガイドライン。

平成17年8月1日に第一版が発行されており、現在、平成25年8月に第三版が発行されている。

（4）国土交通省所管分野における個人情報保護に関するガイドライン

個人情報の保護に関する法律の第七条第一項の規定に基づき定められた「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定）を受け、また同法第八条の規定に基づき国土交通省所管分野における事業者等が講ずべき措置について、適切かつ有効な実施を図るために必要な事項を定めたガイドライン。

平成16年12月2日に国土交通大臣により告示されており、平成27年3月31日に改正されている。

（5）重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針

各重要インフラ事業は、国が定めた安全基準等に従って運用されており、上記指針は重要インフラ13 分野横断的な情報セキュリティ基準を定めたもの。

平成 18 年2月に制定後、現在、平成 27 年 5 月に第4版が発行されている。

2. 鉄道分野における「安全ガイドライン」の概要

2.1 鉄道分野における現状と課題

2.1.1 鉄道分野における情報セキュリティ対策の現状

鉄道分野において、国民生活や社会経済活動に影響を及ぼし事業継続の取り組み対象となるような重要システムには、「列車運行管理システム」、「電力管理システム」及び「座席予約システム」等がある。これらのシステムの障害に対しては、緊急の対応として人手による運用が可能であるものの、代替運用時においては作業効率が低下するため、運行ダイヤが乱れるなどの影響が起こることが想定される。

鉄道分野はその事業特性から、顧客向けのウェブサービス（座席予約等）を保有している事業者も多いが、昨今パスワードリスト攻撃による顧客情報の流出・不正操作というIT障害が発生している。

鉄道分野においては、本「安全ガイドライン」に基づく自己点検、情報セキュリティに関する規程類・対策の策定及び見直し、セキュリティハンドブックの作成・配布及び教育などの対策を実施している事業者もある。

2.1.2 鉄道分野の情報セキュリティ対策における課題

鉄道分野の事業者は、マルウェア感染や外部からの攻撃を防止する対策については各々実施している。しかし、先に述べたパスワードリスト攻撃や標的型攻撃をはじめとする昨今の複雑・巧妙化するサイバー攻撃すべてを防ぐことは困難であるため、攻撃され内部に侵入等されることを前提とした情報セキュリティ対策が必要とされている。

また、一部の事業者では情報セキュリティ対策の継続的改善の取組みが実施されているが、実施が不十分という事業者も多いことが想定されるため、PDCAサイクルに沿った情報セキュリティ対策の継続的改善の実施が必要である。

2.1.3 「安全ガイドライン」の方向性

本「安全ガイドライン」では、分野横断的に有効な対策項目及び対策の例示に加え、鉄道分野における情報セキュリティ対策の現状と課題を踏まえ、事業特性に応じた対策項目を推奨基準としてまとめた。

具体的には、昨今のサイバー攻撃動向や鉄道分野の事業特性に応じた脅威という観点から、標的型攻撃対策、パスワードリスト攻撃対策等を示した。

また、対策項目をPDCAの観点でまとめることで各フェーズで推奨される情報セキュリティ対策を明らかにした。さらに、構築したPDCAのサイクルを円滑に回すことを支援するため、「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第1版）（2015年（平成27年）5月内閣サイバーセキュリティセンター）」を参考文献として示した。

3. 鉄道分野における「安全ガイドライン」の対象範囲等

3.1 「安全ガイドライン」の対象範囲と脅威

3.1.1 「安全ガイドライン」の対象範囲

本「安全ガイドライン」における保護対象は、鉄道分野において、国民生活や社会経済活動への影響が大きく事業継続に対する取り組みの対象となる情報システム及び情報資産(「情報資産」の定義については、「6. 用語集」を参照)である。

例えば、IT 障害の発生によって列車運行の遅延、運休や列車の安全安定輸送に対する支障などの影響を及ぼす以下の重要システム、及びその中で利活用される情報資産が挙げられる。

①列車運行管理システム

列車の運行ダイヤを管理するシステムである。

②電力管理システム

電力の供給設備を管理するシステムである。

③座席予約システム

駅の窓口の端末から座席予約を行うシステムである。

3.1.2 想定する IT 障害の原因

情報セキュリティ対策では、鉄道分野における輸送サービスの継続性の確保を図り、国民の信頼性に応えるとの観点から、意図的な原因、偶発的な原因、環境的な原因といった輸送サービスの提供に影響を及ぼす可能性のある様々な事象を想定し、分野における重要システム及びその運用に関する対応を検討する必要がある。

本「安全ガイドライン」では、重要システムに関連する IT 障害の原因として、以下を想定する。

表　鉄道分野において想定するIT障害の原因

種別	想定するIT障害の原因
意図的な原因	不審メール等の受信、ユーザーID 等の偽り、DoS 攻撃等の大量アクセス、情報の不正取得、内部不正、適切なシステム等運用の未実施　等
偶発的な原因	ユーザーの操作ミス、ユーザーの管理ミス、不審なファイルの実行、不審なサイトの閲覧、外部委託先の管理ミス、機器等の故障、システムの脆弱性、他分野の障害からの波及　等
環境的な原因	災害、疾病　等

3.2 「安全ガイドライン」の運用について

3.2.1 鉄道事業者の担う役割

重要インフラ分野では、国民生活や社会経済活動に重大な影響を及ぼさないように、IT 障害に対する情報セキュリティ対策を適切に行うことが重要である。

その中で重要インフラ事業者の保有する重要なシステム等に係る情報セキュリティの確保については、各事業者が自らの管理下にある情報資産に責任を持ち、それぞれの事業形態や情報システムの形態に適応した情報セキュリティ対策を講じていくことが原則である。

したがって、重要インフラ事業者には、「安全ガイドライン」を適切に参照しながら、自己の対策が十分であるかを自己検証しつつ、必要に応じて情報セキュリティ対策の改善を図ることが求められる。

また情報及び情報システムの取扱いに関しては、法令及び規制等（以下「関連法案等」という）においても規定されているため、情報セキュリティ対策を実施する際には、関連法案等を遵守する必要がある。

3.2.2 「安全ガイドライン」の適用

「安全ガイドライン」は、事業者等が自らの情報セキュリティ対策を実施する際に参考資料として活用することを想定した「推奨基準」であり、「強制基準」ではない。したがって、事業者等にはこの方針を理解したうえで、「安全ガイドライン」の記述に沿った情報セキュリティ確保のための対策を進めることが期待される。

3.2.3 適用状況の評価について

重要インフラ事業者等は、「安全ガイドライン」に対する適用状況等を定期的に点検し、必要に応じて対策の改善を行う必要がある。

重要インフラ事業者が自身の情報セキュリティ対策の妥当性を確認したい場合は、以下を例とする第三者認証制度を活用することを推奨する。

（1）ISMS 適合性評価制度

事業者などの組織が情報を適切に管理し、機密を守るための包括的な枠組みであり、コンピュータシステムに係る情報セキュリティ対策だけでなく、情報を扱う際の基本的な方針としての情報セキュリティポリシーや、それに基づいた具体的な対策の計画・実施・運用、及び見直しまでを含んでいる。

財団法人 日本情報処理開発協会(JIPDEC)が、事業者の ISMS が JIS Q27001:2014 に準拠していることを認証する「ISMS 適合性評価制度」を運用している。

(2) プライバシーマーク制度

日本情報処理開発協会(JIPDEC)が管理する、個人情報取り扱いに関する認定制度である。
個人情報について JIPDEC の定める基準を満たして適正に管理していると認定されれば、使用許諾を得ることができる。審査基準は基本的に JIS Q15001(個人情報保護マネジメントシステム―要求事項)に準拠している。

(3) ITセキュリティ評価及び認証制度

「IT セキュリティ評価及び認証制度 (JISEC)」とは、IT 関連製品のセキュリティ機能の適切性・確実性を、セキュリティ評価基準の国際標準である ISO/IEC 15408 に基づいて第三者(評価機関)が評価し、その評価結果を認証機関が認証する制度である。本制度は主に政府調達において活用されている。

(4) 情報セキュリティ監査制度

情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動のことである。

3.2.4 「安全ガイドライン」の見直し

情報セキュリティの脆弱性は、事業や情報資産を取り巻く環境の変化の影響を受けるものであることから、「安全ガイドライン」については情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行うことが必要である。よって、鉄道分野を始め、国土交通省所管の重要インフラ分野では、「重要インフラ情報セキュリティ対策検討ワーキンググループ」等の活動を通じて、以下のような見直しのための活動を継続していく。

◆ 国土交通省、及び所管する重要インフラ分野の事業者等は、相互に協力し、「安全ガイドライン」について適宜適切なものとなるよう、随時検討を行う。

◆ 国土交通省、及び所管する重要インフラ分野の事業者等は、「安全ガイドライン」の検討及び実効性の確認が容易となるような制度や運営方法について検討を行う。

◆ 国土交通省は、所管する重要インフラ分野の事業者等と協力して、各重要インフラ分野におけるIT障害の発生状況を把握し、当該分野の「安全ガイドライン」に反映されるべき対策項目について検討を行う。

4. 推奨される対策項目

意図的な原因、偶発的な原因、環境的な原因による IT 障害対策について、参考となる対策項目及び推奨事項をそれぞれ記述する。

4.1 「Plan（準備）」の観点

4.1.1 「方針」の観点

4.1.1.1 抽出した課題に基づくリスク評価

【主旨・目的】

情報セキュリティ対策は、日々の情報セキュリティ対策の運用状況に応じて適宜見直さなければ、新たな脅威に対応できない。そのため、情報セキュリティ対策の運用において発見・整理したリスクを考慮し、既存の情報セキュリティ対策を適宜見直す必要がある。

【対策項目】

情報セキュリティ責任者は、4.3「Check(確認)・Act(是正)の観点」で実施したリスク分析の結果に基づき、対応が必要なリスクとその対応の優先順位付けに係る意思決定及び情報セキュリティ対策の策定・見直しに係る基礎情報の作成（リスク評価）を行うこと。

情報セキュリティ責任者は、作成した基礎情報をもとに、リスクの重大性、対応の実現性、リスクの保有状態からのリスクの拡大の可能性も考慮し、情報セキュリティ対策の決定（リスク対応）を行うこと。

4.1.1.2 情報セキュリティ基本方針の策定・見直し

【主旨・目的】

重要インフラ防護のためには、情報セキュリティ対策における根本的な考え方（以下、基本方針）を示す必要がある。

【対策項目】

情報セキュリティ責任者は、重要インフラ防護の目的、目指す方向、情報セキュリティ対策にて守るべき対象等を明らかにし、情報セキュリティへの取組姿勢を基本方針として規定すること。また、基本方針の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても規定すること。

4.1.2 「規定」の観点

4.1.2.1 内規の策定・見直し

【対策の指針】

策定・見直しをした基本方針に基づき、個々の情報セキュリティ対策を体系化した上で、実施に係る考え方、ルール等について策定、見直しを行う。

また、内規の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても策定、見直しを行う。

(1) 情報セキュリティ関係規程の策定・見直し

【主旨・目的】

事業者の情報セキュリティ水準を適切に維持し、情報セキュリティリスクを総合的に低減させるためには、事業者として遵守すべき対策の基準を定めるとともに、情報セキュリティに係るリスク評価の結果を踏まえ、計画的に対策を実施することが重要である。

【対策項目】

情報セキュリティ責任者は、基本方針に準拠した情報セキュリティ関係規程の策定、見直しを行うこと。

なお、内規の策定・見直しに係る主管組織、目的、権限、構成員、見直し要件等についても規程に含めること。

(2) 違反と例外措置

【主旨・目的】

情報セキュリティ違反による損害を最小限に抑えるとともに、違反を今後の対策に活用するため、情報セキュリティ違反を適切な連絡経路をとおして、できるだけ速やかに関係者に報告する必要がある。また、情報セキュリティ違反を犯した取扱者に適用する正式な懲罰手続を確立することが望ましい。

【対策項目】

①違反への対応

情報セキュリティ責任者は、情報セキュリティ関係規程への重大な違反事項に係る報告手続、及び情報セキュリティの維持・改善措置の実施に係る手続、及び取扱者の懲戒手続を整備すること。

②例外措置

情報セキュリティ責任者は、例外措置の適用の申請を審査する者を定め、審査手続を整備すること。

審査者は、例外措置の適用の申請を、定められた手続に従って審査し、許可の可否を決定すること。また、決定の際には、例外措置の審査記録を整備し、保管すること。

例外措置の適用を申請する際には、以下の事項を含む項目を明確にすることが望ましい。

【推奨事項】

＜②に関する推奨事項＞
・ 申請者の情報（氏名、所属、連絡先）
・ 例外措置の適用を申請する情報セキュリティ関係規程の適用箇所（規程名と条項等）
・ 例外措置の適用を申請する期間
・ 例外措置の適用を申請する措置内容（講ずる代替手段等）
・ 例外措置により生じる情報セキュリティ上の影響と対処方法
・ 例外措置の適用を終了したときの報告方法
・ 例外措置の適用を申請する理由

（3） 情報セキュリティ対策の自己点検の計画

【主旨・目的】

情報セキュリティ対策の実効性を担保するためには、情報セキュリティ関係規程の遵守状況等を点検し、その結果を把握・分析することが必要である。

自己点検は、取扱者が自らの役割に応じて実施すべき対策事項を実際に実施しているかどうかを確認するだけではなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要である。

また、自己点検の結果を踏まえ、各当事者は、それぞれの役割の責任範囲において、必要となる改善策を実施する必要がある。

【対策項目】

情報セキュリティ責任者は、自己点検に関し、その実施頻度、実施時期、自己点検すべき項目、実施項目の選択等に関する年度自己点検計画を整備すること。

実施計画には、以下の項目を含む事が望ましい。

【推奨事項】

・ 実施頻度：
年に2度以上実施することが望ましいが、例えば、情報システム部門に対しては、毎月実施し、それ以外の部門に対しては半年に一度の頻度で実施する等、様々な選択肢が考えられる。

・ 実施時期：
例えば、当初は毎月10項目ずつ自己点検し、取扱者の意識が高まった後、半年に一度、全項目を実施するように変更する等、様々な選択肢が考えられる。

・ 確認及び評価の方法：
自己点検が正しく行われていること、自組織の規程に準拠していること、改善すべき事項が改善されていること、対策が有効であること等を評価する。この自己点検の評価においても、数値評価を中心とし、客観性を持った評価とすることが望ましい。例えば、自己点検実施率（対策実施数／自己点検回答数）等の把握が挙げられる。

・ 実施項目：
例えば、前年度に IT 障害が発生した事案や、前年度の自己点検実施率が低かった遵守事項

等、様々な選択肢が考えられる。

(4) 情報セキュリティ対策の監査

【主旨・目的】

情報セキュリティの確保のためには、本ガイドラインに準拠して対策が適切に策定され、かつ運用されることによりその実効性を確保することが重要であって、その準拠性、実効性及び対策の妥当性の有無が確認されなければならない。そのためには、取扱者による自己点検だけでなく、独立性を有する者による情報セキュリティ監査を実施することが必要である。

【対策項目】

情報セキュリティ監査を実施する者は、監査の基本的な方針として、年度情報セキュリティ監査計画を整備すること。また、年度情報セキュリティ監査計画及び情報セキュリティの状況に応じた監査の実施指示に基づき、個別の監査業務毎の監査実施計画を立案すること。

年度情報セキュリティ監査計画には、以下の事項を含むことが望ましい。

【推奨事項】

- 重点とする監査対象及び監査目標(情報漏えい防止、不正アクセス防止など)
- 監査の実施期間
- 監査業務の管理体制
- 外部委託による監査の必要性及び範囲
- 監査に係る予算　等

個別の監査実施計画には、以下の事項を含むことが望ましい

【推奨事項】

- 監査の実施時期
- 監査の実施場所
- 監査の実施担当者及び割当て
- 準拠性監査(情報セキュリティ関係規程に準拠した手続が実施されていることを確認する監査)のほか、必要に応じて妥当性監査(実施している手続が有効な情報セキュリティ対策であることを確認する監査)を行うかについての方針
- 実施すべき監査の概要(監査要点、実施すべき監査の種類及び試査の範囲を含む。)
- 監査の進捗管理手段又は体制

(5) 情報セキュリティ対策の見直し

【主旨・目的】

情報セキュリティを取り巻く環境は常時変化しており、こうした変化に的確に対応しないと、情報セキュリティ水準を維持できなくなる。このため、情報セキュリティ対策の根幹をなす情報セキュリティ関

係規程は、実際の運用において生じた課題、自己点検、監査の結果等を踏まえて、適時見直しを行う必要がある。

【対策項目】

情報セキュリティ責任者は、各規程の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行うこと。見直しを行う時期は、運用段階における事故等の発生、例外措置の申請状況、自己点検・監査の結果、及び取扱者からの相談等により、情報セキュリティ対策に支障が発生しないように判断すること。

見直しを実施するにあたっては、以下の点に留意する事が望ましい。

【推奨事項】

- 見直し手続によって、当初のリスク評価の基礎事項に影響を及ぼす変化（例えば、重大な情報セキュリティの事件・事故、新しい脆弱性、又は組織基盤若しくは技術基盤の変化）に対応して確実に見直しを実施すること。
- 記録された情報セキュリティの事件・事故の性質、回数及び影響によって示される、基本方針の有効性について、日程を定め、定期的に見直しを実施すること。
- 事業効率における管理策の費用及び影響について、日程を定め、定期的に見直しを実施すること。
- 適用する技術の変更による効果について、日程を定め、定期的に見直しを実施すること。

4.1.2.2 IT-BCP 等の策定・見直し

【対策の指針】

本ガイドラインでいう IT-BCP とは、サービス維持レベルを下回る原因となるIT障害発生時等において、情報システムを早期に復旧させ、サービスを継続して提供するために必要な行動手順で構成されるものである。IT障害発生時における優先業務、必要な対策を決定するまでの過程、業務継続方法、連携を要する関連部門等を規定する。

規定に際しては、広域災害・複合障害や新型インフルエンザ等の社会全体で対応が望まれる脅威、相互依存関係にある重要インフラからの障害波及、事業継続に必要なデータが特定の都市又は地域に集中している状況等についても考慮する。

なお、IT障害発生時における適切な対応に向け、平時の事前対策や教育訓練等の実施計画も含む必要がある。

（1） IT 障害の対応

【主旨・目的】

IT 障害が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、IT 障害による影響や範囲を情報セキュリティ責任者へ報告し、IT 障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

【対策項目】

①IT 障害の発生に備えた事前準備

情報セキュリティ責任者は、IT 障害を認知した場合に備え、被害の拡大を防ぐとともに、IT 障害から復旧するために必要な手順（事業者外との情報共有含む）を整備すること。

事前に以下【推奨事項】について整備することが望ましい。

②IT 障害の発生時における報告と応急措置

取扱者は、IT 障害の発生を知った場合には、定められた報告手順により、関係者及び情報セキュリティ責任者にその旨を報告し、状況に応じて定められた適切な応急措置を講ずること。

③IT 障害の原因調査と再発防止策

情報セキュリティ責任者は、取扱者からの IT 障害の原因及び再発防止策についての報告を受けた場合には、その内容を検討し、再発防止策を整備するために必要な措置を指示すること。

【推奨事項】

＜①に関する推奨事項＞
- IT 障害について取扱者からの報告手順
- IT 障害が発生した際の対応手順（応急処置の手順）

（2）情報システムのバックアップ

【主旨・目的】

情報システムは事業を支える重要なインフラとなっており、重要な情報及び情報システムを緊急事態発生時でも使用できることが不可欠である。緊急事態発生時には、通常業務に必要なデータの欠落や不整合による障害が発生するおそれがある。これらを防ぐための詳細な復帰計画をあらかじめ策定しておく必要がある。

【対策項目】

情報セキュリティ責任者は、緊急事態時の事業継続計画の実践時において、代替設備・手段から平常運用へ切り替える際に、通常業務に必要なデータの欠落や不整合による障害の発生を防ぐために、詳細な復帰計画を含む事業継続計画あらかじめ策定しておくこと。

情報セキュリティ責任者は、必要な情報のバックアップを取得し、同じ IT 障害で同時に被災しない場所に保存することはもとより、特に重要な業務を支える情報システムについては、バックアップシステムを整備すること。

情報システムのバックアップに関し、事業継続計画を検討する際には、以下の点を考慮することが望ましい。

【推奨事項】

・守るべき重要業務と情報システムの関係の明確化
・バックアップ稼働・切り替え計画、復帰計画の策定
・自家発電装置、電源や回線など各種設備の二重化対策の実施
・バックアップセンターの設置
・遠隔地の文書・電子データ保存サービスの活用
・バックアップ取得頻度の決定

(3) 事業継続計画(BCP)との整合的運用の確保

【主旨・目的】

事業者においては、事業の継続に重大な支障を来し、あるいは重要インフラ利用者の安全と利益に重大な脅威となる可能性が想定される事態を特定し、当該事態への対応計画を事業継続計画(BCP:Business Continuity Plan)として策定することが考えられる。他方では、BCP の対象とする事態は、多くの場合に情報セキュリティを損なうものともなり、各事業者の情報セキュリティ関係規程に基づく対策も採られることとなる。この場合、BCP の適正な運用と情報セキュリティの確保の双方の目的を適切に達成するためには、両者の整合的運用の確保が必要であるため、BCP と情報セキュリティ対策の整合的運用の確保に関する対策基準を定めることが望ましい。

【対策項目】

①事業者内における BCP 整備計画の把握

情報セキュリティ責任者は、自社における BCP の整備計画について、適時に知ることができる体制を構築すること。

②BCP と情報セキュリティ対策の整合性の確保

情報セキュリティ責任者は、事業者内において BCP 又は事業者内対策基準の整備計画がある場合には、BCP と事業者内対策基準との整合性の確保のための検討を行うこと。

情報セキュリティ責任者は、事業者内において BCP の整備計画がある場合には、すべての情報システムについて、当該 BCP との関係の有無を検討すること。

4.1.2.3 情報の取扱いについての規定化

【対策の指針】

取り扱う情報の重要度に応じて、機密性、完全性、可用性の観点から情報の格付け(ランク付け)を行うとともに、作成、入手、利用、保存、提供、運搬、送信、消去等といった情報のライフサイクルの各段階における遵守事項、情報セキュリティ対策を規定する。

なお、個人データについては、重要インフラ利用者の安心感への影響に鑑みた取扱いを規定する。

(1) 情報の格付け

【主旨・目的】

業務の遂行に当たっては、情報の作成、入手、利用、保存、提供、運搬、送信、消去等を行う必要があり、ある情報のセキュリティの確保のためには、当該情報を利用等する全ての取扱者が情報のライフサイクルの各段階において、当該情報の特性に応じた適切な対策を講ずる必要がある。このため、取扱者は、情報を作成又は入手した段階で当該情報の取扱いについて認識を合わせるための措置として格付及び取扱制限の明示等を行うとともに、情報の格付や取扱制限に応じた対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、業務で取り扱う情報について、電磁的記録については機密性、完全性及び可用性の観点から、書面については機密性の観点から情報の格付け及び取扱制限に関する以下を含む規定を整備し、取扱者へ周知すること。

（ア）情報の格付及び取扱制限についての定義

（イ）情報の格付及び取扱制限の明示等についての手続

（ウ）情報の格付及び取扱制限の継承、見直しに関する手続

(2) 情報のライフサイクルにおける情報セキュリティ対策

(a) 情報の作成・入手

【主旨・目的】

業務の遂行のために複数の者が共通の情報を利用する場合がある。この際、取扱者により当該情報の取扱いに関する認識が異なると、当該情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し又は入手した段階で、すべての取扱者において認識を合わせるための措置が必要となる。

【対策項目】

情報セキュリティ責任者は、情報を作成又は入手することにより発生するリスクに対応するため、情報の作成又は入手時における格付けの決定と取扱制限の明示方法などについて、定められた手順に従って適切な対策を講ずること。

情報の入手と作成については、以下の対策を規定することが望ましい。

【推奨事項】

(1) 業務以外の情報の作成又は入手の禁止
- 取扱者は、業務の遂行以外の目的で、情報システムに係る情報を作成し又は入手しないこと

(2) 情報の作成又は入手時における格付けの決定と取扱制限の検討
- 取扱者は、情報の作成時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること
- 取扱者は、事業者外の者が作成した情報を入手し、管理を開始する時に当該情報の機密性、完全性、可用性に応じて格付けを行い、あわせて取扱制限の必要性の有無を検討すること

(3) 格付けと取扱制限の明示

・ 取扱者は、情報の格付けを、当該情報の参照が許されている者が認識できる方法を用いて明示し、必要に応じて取扱制限についても明示すること
(4) 格付けと取扱制限の継承
・ 取扱者は、情報を作成する際に、既に格付けされた情報を引用する場合には、当該情報の格付け及び取扱制限を継承すること
(5) 格付けと取扱制限の変更
・ 取扱者は、情報の格付けを変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、格付けの見直しを行う必要があると認めた場合には、当該情報に対して妥当な格付けを行うこと
・ 取扱者は、情報の取扱制限を変更する必要性があると思料する場合には、当該情報の作成者又は入手者に相談すること。相談された者は、取扱制限の見直しを行う必要があると認めた場合には、当該情報に対して新たな取扱制限を決定すること

(b) 情報の利用

【主旨・目的】

業務の遂行のために多くの情報を取り扱うが、取扱者の認識不足等による情報の不適切な利用や、情報システムの責任者による脆弱性の対策及び不正プログラム対策の不備等の問題により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれがある。情報を不適切に利用すると、情報の漏えい、改ざん、不当な消去、不当な持出し等によって、情報セキュリティを損なうリスクが増大し、事業に何らかの損害を与えることが考えられる。それらのリスクに対応するため、情報を適切に利用しなければならない。

【対策項目】

情報セキュリティ責任者は、情報を利用することにより発生するリスクに対応するため、情報の取り扱い方法などについて、利用する情報の格付けに応じた適切な対策を講ずること。

情報の利用については、以下の対策を規定することが望ましい。

【推奨事項】

(1) 業務以外の利用の禁止
・ 取扱者は、業務の遂行以外の目的で、情報システムに係る情報を利用しないこと
(2) 格付け及び取扱制限に従った情報の取扱い
・ 取扱者は、利用する情報に明示された格付け及び取扱制限に従って、当該情報を適切に取り扱うこと。

(c) 情報の保存

【主旨・目的】

業務においては、継続性を確保するなどの必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続するため、適切に情報を保存する必要がある。

【対策項目】

情報セキュリティ責任者は、情報を保存することにより発生するリスクに対応するため、情報の管理方法、保存期間等について、保存する情報の格付けに応じた適切な対策を講ずること。

情報の保存については、以下の対策を規定することが望ましい。

【推奨事項】

(1) 格付けに応じた情報の保存
- 情報セキュリティ責任者は、サーバ装置、端末に保存された情報の格付けに従って、適切なアクセス制御を行うこと
- 取扱者は、情報の格付けに従って、情報が保存された外部記録媒体を適切に管理すること
- 取扱者は、情報システムに入力された情報若しくは情報システムから出力した情報を記載した書面について、情報の格付けに従って、適切に管理すること
- 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付けに従って、暗号化を行う必要性の有無を検討し、必要があると認めたときは、客観的に評価された暗号技術※により、情報を暗号化すること
- 取扱者は、情報をサーバ装置、端末又は外部記録媒体に保存する場合には、保存する情報の格付けに従って、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること
- 取扱者は、情報を外部記録媒体に保存する場合には、保存する情報の格付けに従って、外部記録媒体に保存内容が容易に想定できるようなタイトル表示をしない等の対処を行うこと
- 取扱者は、電磁的記録又は設計書等の情報システム関連文書について、情報の格付けに従って、バックアップ又は複写の必要性の有無を検討し、必要があると認めたときは、そのバックアップ又は複写を取得すること
- 情報セキュリティ責任者は、電磁的記録のバックアップ又は設計書等の情報システム関連文書の複写の保管について、情報の格付けに従って、災害等への対策の必要性を検討し、必要があると認めたときは、同時被災等しないための適切な措置を講ずること

※「電子政府推奨暗号リスト」に記載された暗号化アルゴリズム

(2) 情報の保存期間
- 取扱者は、サーバ装置、端末又は外部記録媒体に保存された情報の保存期間が定められている場合には、当該情報を保存期間が満了する日まで保存し、保存期間を延長する必要性がない場合は、速やかに消去すること

(d) 情報の運搬・送信

【主旨・目的】

業務においては、その事務の遂行のために他者又は自身に情報を運搬・送信する場合がある。運搬・送信の方法としては、インターネット上での電子メールや回線接続を通じての送信、情報を格納した外部記録媒体の運搬及びPC、紙面に記載された情報の運搬等の方法が挙げられるが、いずれの方法を用いるにせよ、情報の運搬・送信により、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれが増大することになるため、適切な情報の運搬・送信に係る措置を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、情報を運搬・送信することにより発生するリスクに対応するため、運搬・

送信する情報の形態及び格付けに応じた適切な運搬・送信手段を選択できるように対策を整備すること。

情報の運搬・送信については以下の対策を規定することが望ましい。

【推奨事項】

(1) 情報の運搬・送信に関する許可
・ 取扱者は、情報を運搬・送信する場合には、運搬・送信する情報の格付けに従って、情報セキュリティ責任者の許可を得ること
(2) 情報の送信と運搬の選択
・ 取扱者は、情報を運搬・送信する場合には、運搬・送信する情報の格付けに従って安全確保に留意して、送信又は運搬のいずれによるかを決定すること
(3) 運搬・送信手段の選択
・ 取扱者は、情報を運搬・送信する場合には、運搬・送信する情報の格付けに従って安全確保に留意して、当該情報の運搬・送信手段を決定すること
(4) 書面に記載された情報の保護対策
・ 取扱者は、書面を運搬する場合には、記載されている情報の格付けに従って安全確保のための適切な措置を講ずること

(e) 情報の提供・公表

【主旨・目的】

業務においては、その業務の遂行のために事業者外の者に情報を提供する場合があるが、提供先における情報の不適切な取扱いにより、当該情報の漏えい又は不適切な利用等が発生するおそれがあるため、適切な情報の提供に係る措置を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、情報の提供・公表により発生するリスクに対応するため、提供・公表する情報の形態及び格付けに応じた適切な情報提供・公表がなされるように対策を整備すること。

情報の提供・公表については、以下の対策を規定することが望ましい。

【推奨事項】

(1) 情報の公表
・ 取扱者は、情報を公表する場合には、公表する情報の格付けに従って公表の可否を決定すること
・ 取扱者は、電磁的記録を公表する場合には、情報の格付けに従って、当該情報の付加情報(更新の履歴、文書のプロパティ等をいう。)等からの不用意な情報漏えいを防止するための措置を採ること
(2) 他者への情報の提供
・ 取扱者は、情報を事業者外の者に提供する場合には、提供する情報の格付けに従って、情報セキュリティ責任者の許可を得ること
・ 取扱者は、情報を事業者外の者に提供する場合には、提供先において、提供する情報の格付けに従って適切に取り扱われるよう、取扱い上の留意事項を確実に伝達するなどの措置を講ず

ること
・ 取扱者は、電磁的記録を提供する場合には、情報の格付けに従って、当該記録の付加情報等からの不用意な情報漏えいを防止するための措置を採ること

(f) 情報の消去

【主旨・目的】

業務において利用したサーバ装置、端末、通信回線装置及び外部記録媒体については、不要となった後、適切に処分されずに放置された場合には、盗難や紛失により、記録されている情報が漏えいするおそれがある。また、情報の消去を行ったつもりでも、適切な措置が採られていなければ、復元ツールや復元サービス等を用いて当該情報を復元することが可能であり、情報漏えいのおそれは払拭されないため、適切な情報の消去に係る措置を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、情報の処分により発生するリスクに対応するため、処分する情報の形態及び格付けに応じた適切な処分がなされるように対策を整備すること。

情報の消去については、以下の対策を規定することが望ましい。

【推奨事項】

(1) 電磁的記録の消去方法
・ 取扱者は、電磁的記録媒体に保存された情報が職務上不要となった場合は、速やかに情報を消去すること
・ 取扱者は、サーバ装置、端末、通信回線装置及び外部記録媒体を廃棄する場合には、データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、すべての情報を復元できないよう抹消すること
・ 取扱者は、サーバ装置、端末、通信回線装置及び外部記録媒体を他の者へ提供する場合には、保存された情報の格付けに従って、復元が困難な状態にする必要性の有無を検討し、必要があると認めたときは、データ消去ソフトウェア又はデータ消去装置を用いて、当該サーバ装置、端末等の情報を復元が困難な状態にし、残留する情報を最小限に保つこと
(2) 書面の廃棄方法
・ 取扱者は、情報が記録された書面を廃棄する場合には、廃棄する情報の格付けに従って、復元が困難な状態にすること

(3) 個人情報保護に関わる対策

【主旨・目的】

業務で取り扱う個人情報については、その目的、用途及び保管項目により、取扱いに慎重を要する度合いは様々であり、その重要性に応じた適切な措置を講じ、確実に情報セキュリティを確保するために、適切な対策を講ずる必要がある。

【対策項目】

①個人データ取り扱い台帳の整備

情報セキュリティ責任者は、個人データについて、取得する項目、明示・公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備し、定期的に内容を更新することで最新状態を維持すること。

②個人情報の類型化

情報セキュリティ責任者は、個人データの適切なレベルでの保護を確実にし、保護の必要性、優先順位、及び程度を示すために、漏えい時の事業への影響度などのリスク評価の結果に応じて分類すること。

(4) 個人情報に関わる管理

【主旨・目的】

業務の遂行のために複数の者が共通の個人情報を利用する場合がある。この際、取扱者により個人情報の取扱いに関する認識が異なると、個人情報に応じた適切な情報セキュリティ対策が採られないおそれがあるため、情報を作成し又は入手した段階で、すべての取扱者において認識を合わせるための措置が必要となる。

【対策項目】

①データ内容の正確性の確保

情報セキュリティ責任者は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つこと。

②ライフサイクルに基づいた個人情報の管理対策

情報セキュリティ責任者は、個人情報が記録された媒体を、ライフサイクル(「取得・入力」「運搬・送信」「利用・加工」「保管・バックアップ」「消去・廃棄」)に基づいて適切に取り扱うための措置を明示すること。

ライフサイクルに基づいた個人情報の管理対策を検討する際には、以下【推奨事項】の対策を講ずることが望ましい。

【推奨事項】

＜②に関する推奨事項＞
(1) 個人情報の取得・入力
・ 作業責任者の明確化
　－個人データを取得する際の作業責任者の明確化
　－取得した個人データを情報システムに入力する際の作業責任者の明確化
・ 手続の明確化と手続に従った実施

－取得・入力する際の手続の明確化
－定められた手続による取得・入力の実施
－権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）での入力作業の実施
－個人データを入力できる端末の、業務上の必要性に基づく限定
－個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）

・ 作業担当者の識別、認証、権限付与
－個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
－ID とパスワードによる認証、生体認証等による作業担当者の識別
－作業担当者に付与する権限の限定
－個人データの取得・入力業務を行う作業担当者に付与した権限の記録

・ 作業担当者及びその権限の確認
－手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
－アクセスの記録、保管と、権限外作業の有無の確認

(2) 運搬・送信

・ 作業責任者の明確化
－個人データを運搬・送信する際の作業責任者の明確化

・ 手続の明確化と手続に従った実施
－個人データを運搬・送信する際の手続の明確化
－定められた手続による運搬・送信の実施
－個人データを運搬・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆回線を利用して個人データを送信する場合）
－運搬時におけるあて先確認と受領確認（例えば、簡易書留郵便その他個人情報が含まれる荷物を輸送する特定のサービスの利用）
－FAX等におけるあて先番号確認と受領確認
－個人データを記した文書をFAX等に放置することの禁止
－暗号鍵やパスワードの適切な管理

・ 作業担当者の識別、認証、権限付与
－個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
－ID とパスワードによる認証、生体認証等による作業担当者の識別
－作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。）
－個人データの移送・送信業務を行う作業担当者に付与した権限の記録

・ 作業担当者及びその権限の確認
－手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
－アクセスの記録、保管と、権限外作業の有無の確認

(3) 利用・加工

・ 作業責任者の明確化
－個人データを利用・加工する際の作業責任者の明確化

・ 手続の明確化と手続に従った実施
－個人データを利用・加工する際の手続の明確化
－定められた手続による利用・加工の実施
－権限を与えられていない者が立ち入れない建物等での利用・加工の実施

－個人データを利用・加工できる端末の、業務上の必要性に基づく限定
－個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）

・ 作業担当者の識別、認証、権限付与
－個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
－ID とパスワードによる認証、生体認証等による作業担当者の識別
－作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）
－個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

・ 作業担当者及びその権限の確認
－手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
－アクセスの記録、保管と権限外作業の有無の確認

(4) 保管・バックアップ

・ 作業責任者の明確化
－個人データを保管・バックアップする際の作業責任者の明確化

・ 手続の明確化と手続に従った実施
－個人データを保管・バックアップする際の手続※の明確化
※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（OS）やアプリケーションのバックアップも必要となる場合がある。

・ 定められた手続による保管・バックアップの実施
－個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化
－暗号鍵やパスワードの適切な管理
－個人データを記録している媒体を保管する場合の施錠管理
－個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
－個人データを記録している媒体の遠隔地保管
－個人データのバックアップから迅速にデータが復元できることのテストの実施
－個人データのバックアップに関する各種事象や障害の記録

・ 作業担当者の識別、認証、権限付与
－個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
－ID とパスワードによる認証、生体認証等による作業担当者の識別
－作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。）
－個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

・ 作業担当者及びその権限の確認
－手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
－アクセスの記録、保管と権限外作業の有無の確認

(5) 消去・廃棄

・ 作業責任者の明確化
－個人データを消去する際の作業責任者の明確化
－個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

・ 手続の明確化と手続に従った実施
－消去・廃棄する際の手続の明確化

－定められた手続による消去・廃棄の実施
－権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
－個人データを消去できる端末の、業務上の必要性に基づく限定
－個人データが記録された媒体や機器をリース事業者に返却する前の、データの完全消去（例えば、意味のないデータを媒体に1回又は複数回上書きする。）
－個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）
・ 作業担当者の識別、認証、権限付与
－個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定
－ID とパスワードによる認証、生体認証等による作業担当者の識別
－作業担当者に付与する権限の限定
－個人データの消去・廃棄を行う作業担当者に付与した権限の記録
・ 作業担当者及びその権限の確認
－手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
－アクセスの記録、保管、権限外作業の有無の確認

(5) 不正アクセスのための脅威への対策

【主旨・目的】

個人情報が保存されたPCや外部記録媒体の盗難、紛失及び当該PCや外部記録媒体からの情報漏えいを防止するための措置や、個人情報を処理するアプリケーションからの情報漏えいを防止するために、適切な対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない。

その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講ずること。

不正アクセスのための脅威への対策を検討する際には、以下の対策を講ずることが望ましい。

【推奨事項】

① 組織的安全管理措置
情報セキュリティ責任者は、安全管理について取扱者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認すること
・ 個人データの安全管理措置を講ずるための組織体制の整備
・ 個人データの安全管理措置を定める規程等の整備と規程等に従った運用
・ 個人データの取扱い状況を一覧できる手段の整備
・ 個人データの安全管理措置の評価、見直し及び改善
・ 事故又は違反に対する対処
② 人的安全管理措置

情報セキュリティ責任者は、取扱者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うこと
・ 雇用契約時及び委託契約時における非開示契約の締結
・ 取扱者に対する内部規程等の周知・教育・訓練の実施
③技術的安全管理措置
情報セキュリティ責任者は、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置を講ずること
・ 個人データへのアクセスにおける識別と認証
・ 個人データへのアクセス制御
・ 個人データへのアクセス権限の管理
・ 個人データのアクセスの記録
・ 個人データを取り扱う情報システムについての不正ソフトウェア対策
・ 個人データの運搬・送信時の対策
・ 個人データを取り扱う情報システムの動作確認時の対策
・ 個人データを取り扱う情報システムの監視
④物理的安全管理措置
情報セキュリティ責任者は、入退館(室)の管理、個人データの盗難の防止等の措置を講ずること
・ 入退館(室)管理の実施
・ 盗難等の防止
・ 機器・装置等の物理的な保護

(6) 内部関係者による脅威への対策

(a) 事業者外での情報処理の制限

【主旨・目的】

業務の遂行のため、事業者外において情報処理を実施する必要が生ずる場合がある。この際、事業者外での実施では物理的な安全対策を講ずることが比較的困難になることから、取扱者は、事業者内における安全対策に加え、追加の措置が必要であることを認識し、適切な対策に努める必要がある。

【対策項目】

情報セキュリティ責任者は、事業者外での情報処理を行う場合、及び情報システムを事業者外に持ち出す場合の安全管理措置について、対象となる情報の格付けに従って、規定を整備すること。この際、申請者を審査するために必要な手続を明確に規定すること。

事業者外での情報処理及び情報システムを事業者外に持ち出す場合について、以下を規定することが望ましい。

【推奨事項】

・ 取扱者は、事業者外で情報処理を行う場合、及び情報システムを事業者外に持ち出す場合は、取扱う情報の格付けに従って、情報セキュリティ責任者の許可を得ること
・ 取扱者は、事業者外で情報処理を行う場合は、取扱う情報の格付けに従って、必要な安全管理措置を講ずること。

(b) 事業者支給以外の情報システムによる情報処理の制限

【主旨・目的】

業務においては、その遂行のため、事業者支給以外の情報システムを利用する必要が生じる場合がある。この際、当該情報システムが、事業者が支給したものでないという理由で対策を講じなかった場合、当該情報システムで取り扱われる情報のセキュリティは確保できないため、適切な対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、事業者支給以外の情報システムにより情報処理を行う場合に講ずる安全管理措置について、処理の対象となる情報の格付けに従って、端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための必要な対策を講ずること。この際、申請者を審査するために必要な手続を明確に規定すること。

(c) 取扱者の管理

【主旨・目的】

個人情報の漏えい事故の多くは取扱者などの内部関係者による、内部犯行となっていることから、内部関係者の個人情報保護に対する意識を高め情報漏えいを抑止するために、取扱者の適正な管理を行うことが必要である。

【対策項目】

①安全管理措置

情報セキュリティ責任者は、取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの保護のため、組織的、人的、物理的及び技術的安全管理措置を講ずること。その際、本人の個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況並びに個人データを記録した媒体の性質等に起因するリスクに応じ、必要かつ適切な措置を講ずること。

②取扱者の監督

情報セキュリティ責任者は、個人データの安全管理が図られるよう、取扱者に対し必要かつ適切な監督をしなければならない。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、個人データを取り扱う取扱者に対する教育及び研修等の内容及び頻度を充実させるなど、必要かつ適切な措置を講ずること。

取扱者のモニタリングを実施する際には、以下【推奨事項】のような対策を講ずることが望ましい。

③雇用管理

情報セキュリティ責任者は、取扱者を雇用する場合、4.1.2.3(3)に規定する安全管理措置を取扱者に実施させることを契約条件とする等、以下【推奨事項】を例とする必要かつ適切な措置を講ずること。

【推奨事項】

＜②に関する推奨事項＞
- モニタリングにおいて取得する個人情報の利用目的をあらかじめ特定し、事業者内規程に定めるとともに、取扱者に明示すること。
- モニタリングの実施に関する責任者とその権限を定めること
- モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた事業者内規程案を策定するものとし、事前に事業者内に徹底すること
- モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと

＜③に関する推奨事項＞
- 雇用契約時における情報の守秘や非開示の契約の締結
- 退職後の個人情報保護規定の整備

(7) 個人情報漏えい発生時の対応策の整備

【主旨・目的】

個人情報の漏えいが発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、IT 障害による影響や範囲を定められた関係者へ報告し、IT 障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

【対策項目】

① 個人データ漏えい発生時の対応

情報セキュリティ責任者は、個人データの漏えい等が発生した場合はまず、漏えい源の特定、漏えい継続の阻止、関係機関への周知、漏えいした情報の拡散阻止等の対策を取ること。

その後、個人データ漏えいに至った経緯、原因等の解析を行い、再発防止策を検討し、対策を施すこと。

② 本人への通知

情報セキュリティ責任者は、個人データの漏えい等が発生した場合に、事実関係を本人に速やかに通知するために必要な手続を規定すること。

③ 事実関係、再発防止策等の公表

情報セキュリティ責任者は、個人データの漏えい等が発生した場合に、二次被害の防止、類似事案の発生回避等の観点から、可能な限り影響範囲などの事実関係、再発防止策等を公表するために必要な手続を整備すること。

④ 国土交通省への報告

情報セキュリティ責任者は、個人データの漏えい等が発生した場合に、事実関係を国土交通省に直ちに報告するために必要な手続を整備すること。

4.1.3 「計画」の観点

(1) 情報セキュリティ対策に係るロードマップ及び計画の作成・見直し

情報セキュリティ責任者は、方針の策定・見直し等に基づき、情報セキュリティ対策の具体的な達成目標が定め、達成までの大まかなスケジュールであるロードマップ及びロードマップに基づき詳細化した計画を作成し、情報セキュリティ対策を進めること。

4.1.4 「体制」の観点

4.1.4.1 予算・体制(委託先を含む)の確保

【対策の指針】

情報セキュリティ対策を計画に沿って進めるにあたり、情報システムの構築・運用及び当該方針の実行に必要な予算・体制・人材等の経営資源を継続的に確保する。

(1) 組織・体制の確立

【主旨・目的】

情報セキュリティ対策は、それに係るすべての者が、職制及び職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。そのため、それらの権限と責務を明確にし、必要となる組織・体制を確立する必要がある。

【対策項目】

①組織・体制の確立

鉄道事業者は、情報システムの情報セキュリティを推進する組織又は体制を構築するとともに、情報システム及び情報資産について、その保護並びに情報セキュリティ確保の活動に関する管理及び指導を行う者(以下、「情報セキュリティ責任者」という。)を定めること。

鉄道事業者は、情報システムの管理又は操作を行う者(以下、「取扱者」という。)について、情報セキュリティに対する責任を定めること。

②役割・責任分担の確立

事業者は、情報セキュリティ対策の実施にあたり、適切な責任分担及び十分な資源配分によって、情報セキュリティを促進することが必要であることから、個々の資産の保護に対する責任及び特定の情報セキュリティ手続の実施に対する責任及び役割を、明確に定めること。

また、必要に応じて外部専門家の登用を検討すること。

(2) 役割の分離

【主旨・目的】

情報セキュリティ対策に係る組織において、承認する者と承認される者が同一である場合や、監査する者と監査される者が同一である場合は、情報セキュリティが確保されていることが確認、証明されたことにはならない。情報セキュリティを確立するためには、兼務してはいけない役割が存在するため、情報セキュリティ対策に係る職務については分離に関する規程を設ける必要がある。

【対策項目】

情報セキュリティ責任者は、情報セキュリティ対策の運用において、「承認又は許可事案の申請者とその承認者又は許可者」及び「監査を受ける者とその監査を実施する者」の職務について同じ者が兼務しないよう規程を整備すること。

(3) IT 障害の対応

(a) IT 障害発生時の体制の整備

【主旨・目的】

IT 障害が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。また、その際には、IT 障害による影響や範囲を情報セキュリティ責任者へ報告し、IT 障害の発生現場の混乱や誤った指示の発生等を最小限に抑えることが重要である。

【対策項目】

情報セキュリティ責任者は、IT 障害を認知した場合に備え、被害の拡大を防ぐとともに、IT 障害から復旧するために必要な体制を整備すること。

事前に以下の事項について規程を整備することが望ましい。

【推奨事項】

- 業務の遂行のため特に重要と認めた情報システムにおける、担当する情報セキュリティ責任者の緊急連絡先、連絡手段、連絡項目を含む緊急連絡網

(b) 対外的な情報発信及び情報共有

【主旨・目的】

緊急事態発生後は、事業者活動が関係者から見えなくなる、何をしているのか全然わからないといった、いわゆるブラックアウトを防ぐための対策を講ずる必要がある。そのためにも、関係者との事前の協議が必要となる。

【対策項目】

情報セキュリティ責任者は、緊急事態発生後に、取引先、顧客、従業員、株主、地域住民、政府・自治体などと情報を共有するために以下の点を含む事業継続計画を検討すること。

【推奨事項】

- 情報収集・伝達、広報体制を確立すること
- 関係当局、周辺住民、サプライチェーン等の関係者との連絡体制を構築すること
- 通信・情報連絡手段を確保すること

(4) 事業継続性確保のための指揮命令系統の明確化

【主旨・目的】

事業継続の取組みの推進や災害発生等の緊急事態の対応には、責任の所在を明確にして対策に取り組む必要があるため、事業継続の組織体制の構築とその役割及び指揮命令系統を明確にしておく必要がある。

【対策項目】

情報セキュリティ責任者は、事業継続の取組みの推進や災害発生等の緊急事態の対応には、事業継続の組織体制の構築とその役割及び指揮命令系統を明確にすること。また、非日常的な業務を実施するために必要な経営資源を明確化し、調達の必要性を判断すること。

指揮命令系統の明確化に関し、事業継続計画を検討する際には、以下の点を考慮することが望ましい。

【推奨事項】

- 緊急事態時の組織体制について、緊急時対策本部長、事務局、各部門の対策実施本部などを組織化すること
- 緊急事態時には日常の業務と全く異なる業務が発生するため、部門を越えた動員体制を構築しておくこと
- 緊急時対策の責任者に連絡が付かなかった場合や不在の場合の権限委譲や代行順位をあらかじめ決定しておくこと
- 各部門の対策実施の責任者についても権限委譲や代行順位を決定すること

4.1.4.2 人材育成・配置・ノウハウの蓄積

【対策の指針】

システムにおける情報セキュリティ対策は複数の対策を組み合わせることで成り立っているケースが多い。また、平時のシステム保守においても組織やシステムユーザーの変更、システムのチューニング等といった情報セキュリティ対策の水準を維持するための対応が必要である。

このことから、情報セキュリティ対策に係る担当者が変更となっても情報セキュリティ対策の水準を維持できるよう、ノウハウを蓄積するとともに、実効性を考慮した継続的な人材育成と配置を行う。

また、情報セキュリティに係る教育は、システム業務に従事する人材のみならず、システムユーザーやPC操作者も対象であることから、全社的に行う。

【主旨・目的】

規程が適切に整備されているとしても、その内容が取扱者に周知されず、これが遵守されない場合には、情報セキュリティ水準の向上を望むことはできない。このため、全ての取扱者が、情報セキュリティの教育を通じ、規程への理解を深め、情報セキュリティ対策を適切に実施することが必要である。

【対策項目】

情報セキュリティ責任者は、情報セキュリティ関係規程について、取扱者を適切に教育・配置するための計画を立案するとともに、その実施体制及び教育のための資料を整備し、ノウハウの蓄積に努めること。

教育内容としては、以下のような項目を含むことが望ましい。

【推奨事項】

- 情報の取扱い（格付け及び取扱制限）
- 情報セキュリティポリシー
- 情報セキュリティへの脅威と対策
- IT 障害発生時の対処手順及び体制

4.1.4.3 外部委託における対策（管理体制・契約・IT 障害時）

【対策の指針】

重要情報の漏えいや悪意のあるシステム操作等については、外部からの意図的な原因のみならず内部の意図的又は偶発的な原因にて生じることがある。この内部の意図的又は偶発的な原因は、重要インフラ事業者等の従業員のみならず、委託先によるものも含まれる。

このことから、外部委託先に係る管理体制については、外部委託の適否及びその可能な範囲の明確化や委託先の選定基準に基づく外部委託契約、外部委託先の業務管理等にて行う。特に従業員と同じレベルの情報セキュリティ対策や教育の実施、IT障害発生時の協力についての合意は必要である。

（1） 委託先管理の仕組み

【主旨・目的】

事業者の外部の者に情報システムの開発、アプリケーションプログラムの開発等を委託する際、取扱者が当該委託先における情報セキュリティ対策を直接管理することができないため、事業者内部で行う場合と比べ、情報の機密性、完全性及び可用性が損なわれるリスクが増大する。

このリスクに対応するため、情報システムの開発、アプリケーションプログラムの開発等を外部委託する際は、委託先においても事業者内基準と同等の対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

【対策項目】

①事業者内における情報セキュリティ確保の仕組みの整備

情報セキュリティ責任者は、外部委託を認める情報システムの範囲を整備するとともに委託先によるアクセスを認める情報及び情報システムの範囲を判断する基準、委託先の選定手続・選定基準、及び委託先が具備すべき要件（委託先従業員に対する情報セキュリティ対策の実施を含む）を整備すること。

委託先の選定基準には、以下【推奨事項】を例とする条件を含めることが望ましい。

②委託先に適用する情報セキュリティ対策の整備

情報セキュリティ責任者は、外部委託に係る業務遂行に際して、委託先に実施させる情報セキュリティ対策の内容を整備し、調達仕様書等に定め、委託の際の契約条件とすること。

③個人情報を委託する場合の対策

情報セキュリティ責任者は、適切な委託先管理を実施するために、個人データの安全管理、取扱い時の報告義務、責任の範囲、及び非開示義務について、委託契約時に明確にすべき内容を規定すること。

契約時に明確にする項目について、以下【推奨事項】の対策を講ずることが望ましい。

【推奨事項】

＜①に関する推奨事項＞
- 委託先に提供する情報の委託先における目的外利用の禁止
- 委託先における情報セキュリティ対策の実施内容及び管理体制
- 委託先企業又はその従業員、再委託先、若しくはその他の者による意図せざる変更が加えられないための管理体制
- 委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
- IT 障害に対する対処方法
- 情報セキュリティ対策その他の契約の履行状況の確認方法
- 情報セキュリティ対策の履行が不十分な場合の対処方法

＜③に関する推奨事項＞
- 個人データの安全管理に関する事項
  －個人データの漏えい等の防止、盗用の禁止に関する事項
  －委託契約範囲外の加工、利用の禁止
  －委託契約範囲外の複写、複製の禁止
  －委託期間
  －委託終了後の個人データの返還・消去・破棄に関する事項
- 個人データの取扱いの再委託を行うに当たっての委託元への報告とその方法
- 個人データの取扱い状況に関する委託者への報告の内容及び頻度
- 委託契約の内容、期間が遵守されていることの確認
- 委託契約の内容、期間が遵守されなかった場合の措置
- 個人データの漏えい等の事故が発生した場合の報告・連絡に関する事項

・ 個人データの漏えい等の事故が発生した場合における委託元と委託先の責任の範囲

(2) 外部委託実施における情報セキュリティ確保策の徹底

【主旨・目的】

情報システムの開発、アプリケーションプログラムの開発等を外部委託する際は、委託先選定、委託の実施において必要な対策を講ずる必要がある。

【対策項目】

①外部委託先の選定における手続の遵守

情報セキュリティ責任者は、整備されている選定手続、選定基準及び委託先が具備すべき要件に基づき、委託先を選定すること。

②外部委託の実施における手続の遵守

情報セキュリティ責任者は、外部委託を実施する際に、委託先に請け負わせる業務における情報セキュリティ対策、機密保持(情報の目的外利用の禁止を含む。)、IT 障害に対する対処手順及び情報セキュリティ対策の履行が不十分である場合の対処手順を含む外部委託に伴う契約を取り交わすこと。

外部委託の実施における手続としては、以下【推奨事項】の対策を講ずることが望ましい。

③外部委託終了時の手続の遵守

情報セキュリティ責任者は、外部委託の終了時に、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること。

④個人情報を委託する場合の委託先の監督

情報セキュリティ責任者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行うこと。その際、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、委託する事業の規模及び性質並びに個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。

【推奨事項】

＜②に関する推奨事項＞

・ 情報セキュリティ責任者は、外部委託に係る契約者双方の責任の明確化と合意の形成を行い、委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書を提出させること
・ 情報セキュリティ責任者は、委託先がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、本項に規定する情報セキュリティ対策の実施を委託先に担保させること

・ 取扱者は、委託先に提供する情報を必要最低限とし、委託先が取り扱う情報の格付けに従って、適切な情報セキュリティ対策を講ずること
・ 情報セキュリティ責任者は、情報システムの構築、運用・保守を外部委託する場合には、委託先が実施すべき対策事項を検討し、当該対策事項が実質的に担保されるよう、委託先に実施について保証させること

(3) IT 障害発生時の対応策の整備

【主旨・目的】

IT 障害が発生した場合には、早急にその状況を検出し、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。このため、委託先に請け負わせる業務における IT 障害に対する対処手順を明確に定めておくことが重要である。

【対策項目】

情報セキュリティ責任者は、委託先に請け負わせる業務においてIT障害を認知した場合の対処手順を整備すること。

4.1.5 「構築」の観点

4.1.5.1 情報セキュリティ要件の明確化・変更

【対策の指針】

重要インフラ事業者等が有する情報システムへの情報セキュリティ対策の実装に向け、機密性、完全性、可用性等の観点から、導入を要する情報セキュリティ機能を明示する。

その際、ソフトウェアに関する脆弱性、不正プログラム、DoS 攻撃等の様々な脅威に対して導入を要する情報セキュリティ機能、未然防止対策及びIT障害発生後の拡大防止・早期復旧の対策に要する機能をできる限り明示するとともに、そもそもの不正侵入を防止するための対策と許してしまった侵入がもたらす実被害を防止するための対策についても明示する。

(1) 不正侵入防止対策

(a) 主体認証機能

【主旨・目的】

情報システムの利用においては、その利用主体の識別と主体認証を可能とする機能がない場合、本来アクセス権限のない者が、悪意又は過失により、情報の参照、改ざん又は消去を行うおそれがあるため、情報システムが取り扱う情報の格付けに従った適切な主体認証を実施する必要がある。

【対策項目】

①主体認証機能の導入

情報セキュリティ責任者は、情報システムについて、情報の格付けに従って、識別及び主体認証を行う機能を設けること。この際、認可されていないアクセスのおそれを最小限に抑えるため、採用する認証技術や識別コード・主体認証情報の安全管理措置について、適切に設計すること。

②取扱者の責任

情報セキュリティ責任者は、取扱者が、識別コード及び主体認証情報の使用及び管理について、正しいセキュリティ慣行に従うように、自分自身の責任を認識させること。特にパスワードの使用及び取扱者が利用する端末装置のセキュリティに関して、その責任を十分に認識させること。

取扱者における識別コード・主体認証情報の管理対策としては、以下の対策を規定することが望ましい。

【推奨事項】

＜②に関する推奨事項＞
- 取扱者は、自己に付与された識別コード以外の識別コードを用いて、情報システムを利用しないこと
- 取扱者は、自己に付与された識別コードを他者に付与及び貸与しないこと
- 取扱者は、自己に付与された識別コードを、それを知る必要のない者に知られるような状態で放置しないこと
- 取扱者は、業務のために識別コードを利用する必要がなくなった場合は、情報セキュリティ責任者に届け出ること
- 取扱者は、主体認証情報としてパスワードを設定する場合、以下の要素を考慮して、セキュリティ上の強度が高くなるようパスワードを設定すること
  - パスワードに用いる文字の種類とその組み合わせ
  - パスワードの桁数
  - パスワードの有効期間
- 取扱者は、主体認証情報が他者に使用され又はその危険が発生した場合には、直ちに情報セキュリティ責任者にその旨を報告すること

（b）アクセス制御機能

【主旨・目的】

情報システムを複数の者が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの者がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

【対策項目】

①アクセス制御機能の導入

情報セキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討して、アクセス制御を行う機能を設けること。

②取扱者による適切なアクセス制御

取扱者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。

（c）権限管理機能

【主旨・目的】

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのアクセスを許してしまうことになるため、権限管理を行う必要がある。

【対策項目】

情報セキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討し、権限管理を行う機能を設けること。この際、取扱者への識別コード及び主体認証情報の付与に関する手続を明確に定めること。

権限管理について、以下の事項を含む手続を明確にすることが望ましい。

【推奨事項】

- 主体からの申請に基づいて権限管理を行う場合には、その申請者が正当な主体であることを確認するための手続
- 主体認証情報の初期配布方法及び変更管理手続
- アクセス制御情報の設定方法及び変更管理手続

(d) 暗号と電子署名(鍵管理を含む)

【主旨・目的】

情報システムの利用においては、情報システムで取り扱う情報の漏えい、改ざん等を防ぐための手段として、暗号と電子署名は有効であり、情報システムにおける機能として適切に実装する必要がある。

【対策項目】

①暗号化機能及び電子署名の付与機能の導入

情報セキュリティ責任者は、情報システムについて、システムが保有する情報の格付けに従って、暗号化機能(機密性の保護)、及び電子署名の付与機能(電子文書の完全性の保護)の必要性の有無を検討し、必要な機能を導入すること。また、暗号化又は電子署名の付与に用いるアルゴリズムを選択するに当たっては、その暗号強度、利用条件、効率性等について多角的な検討を行うこと。

②暗号化及び電子署名の付与に係る管理

情報セキュリティ責任者は、暗号化又は電子署名の付与を行う必要があると認めた情報システムにおいて、暗号化された情報の復号又は電子署名の付与に用いる鍵について、鍵の保存方法の生成手順、有効期限、廃棄手順、更新手順、鍵が露呈した場合の対応手順等を定めること。

暗号化機能及び電子署名の付与機能の利用については、以下の対策を講ずることが望ましい。

【推奨事項】

＜①、②に関する推奨事項＞
- 取扱者は、情報を運搬・送信する場合又は電磁的記録媒体に保存する場合には、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること。
- 取扱者は、情報を運搬・送信する場合又は電磁的記録媒体に保存する場合には、電子署名の付与を行う必要性の有無を検討し、必要があると認めたときは、情報に電子署名を付与すること
- 取扱者は、暗号化された情報の復号又は電子署名の付与に用いる鍵について、これを他者に知られないように自己管理すること
- 取扱者は、暗号化された情報の復号に用いる鍵について、機密性、完全性、可用性の観点から、バックアップの必要性の有無を検討し、必要があると認めたときは、そのバックアップを取得し、オリジナルの鍵と同等の安全管理をすること

（e）ソフトウェアに関する脆弱性対策

【主旨・目的】

ソフトウェアに関する脆弱性は、情報システムを構成するサーバ装置、端末及び通信回線装置上で利用しているソフトウェアに存在する可能性があり、その脆弱性を攻撃者に悪用されることにより、サーバ装置への不正侵入、サービス不能攻撃、ウィルス感染等の脅威の発生原因になるなど、情報システム全体のセキュリティの大きな脅威となる。特に、サーバ装置へ不正侵入された場合、踏み台、情報漏えい等の更なるリスクにつながり、事業者の社会的な信用が失われるおそれがある。これらのリスクを回避するため、ソフトウェアに関する脆弱性への対応は迅速かつ適切に行う必要がある。

【対策項目】

情報セキュリティ責任者は、サーバ装置、端末及び通信回線装置上で利用しているソフトウェアについて、当該ソフトウェアに関する脆弱性対策に必要となる情報を収集すること。

情報セキュリティ責任者は、サーバ装置、端末及び通信回線装置の構築又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

（f） 不正プログラム対策

【主旨・目的】

不正プログラムは、これに感染した情報システム及びデータを破壊することから完全性、可用性に対する脅威となるだけでなく、主体認証情報等の秘密情報や業務上の機密情報を漏えいさせることから機密性に対する脅威ともなる。さらに、不正プログラムに感染した情報システムは、他の情報システムの再感染を引き起こす危険性のほか、迷惑メールの送信やサービス不能攻撃等の踏み台として利用される危険性など他者に対するセキュリティ脅威の原因となり得る。よって、不正プログラム対策を行う必要がある。

【対策項目】

情報セキュリティ責任者は、不正プログラム感染の回避を目的とした取扱者に対する留意事項を含む日常的実施事項を定めること。

また、情報セキュリティ責任者は、サーバ装置、端末及び想定される不正プログラムの感染経路の全てにおいて不正プログラム対策ソフトウェア等を導入すること。

(2) 実被害防止対策

(a) ログの取得・管理

【主旨・目的】

情報システムにおけるログとは、システムの動作履歴、取扱者のアクセス履歴、その他必要な情報が記録されたものであり、悪意ある第三者等による不正侵入や不正操作等の IT 障害(その予兆を含む。)を検知するための重要な材料となるものである。また、情報システムに係る情報セキュリティ上の問題が発生した場合には、当該ログは、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログが取得され、また、改ざんや消失等が起こらないよう、ログが適切に保全されなければならない。

【対策項目】

①ログの取得

情報セキュリティ責任者は、すべての情報システムについて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行う必要性の有無を検討し、ログを取得すること。また、情報セキュリティ責任者は、事象をログとして記録するに当たり、事象ごとに必要な情報項目を記録するように、情報システムの設定をすること。

ログとして記録する項目としては、以下【推奨事項】の事項を含めることが望ましい。

②取得したログの点検、分析及び報告

情報セキュリティ責任者は、取得したログを定期的に又は適宜点検及び分析し、その結果に応じて必要な情報セキュリティ対策を講ずること。

【推奨事項】

＜①に関する推奨事項＞
- 事象の主体である人又は機器を示す識別コード
- 識別コードの発行等の管理記録
- 取扱者等による情報システムの操作記録
- 事象の種類(ウェブサイトへのアクセス、ログオン及びログアウト、ファイルへのアクセス、アプリケーションの起動及び終了、特定の操作指令等)
- 事象の対象(アクセスした URL(ウェブアドレス)、ログオンしたアプリケーション、アクセスしたファイル、起動及び終了したアプリケーション、操作指令の対象等)
- 日付、時刻
- 成功、失敗の区別、事象の結果
- 電子メールのヘッダ情報、通信内容
- 通信パケットの内容
- 操作員、監視要員及び保守要員等への通知の内容

(b) 負荷分散・冗長化

【主旨・目的】

重要システムの停止・低下は、国民生活や社会経済活動に重大な影響を及ぼすことから、障害や過度のアクセス等によりサービスが提供できない事態となることを防がなければならない。障害や過度のアクセス等、将来の見通しも考慮し、サービス提供に必要なサーバ装置等を冗長構成にするなどにより可用性を確保する必要がある。

【対策項目】

情報セキュリティ責任者は、トラフィックの集中や一部の装置の不具合によるシステム機能停止を予防するため、システムの負荷分散や冗長化について検討を行い、必要があると認められる場合は、二重化を図るなど適切に処置を行うこと。

(c) サービス不能攻撃対策

【主旨・目的】

インターネットを経由して外部に提供しているサービスを実現する情報システムは、第三者からサービス不能攻撃を受け、重要インフラ利用者がサービスを利用できなくなるという脅威が想定される。このため、インターネットからアクセスを受ける情報システムについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施する必要がある。

【対策項目】

情報セキュリティ責任者は、情報システム(インターネットからアクセスを受けるサーバ装置、端末及び通信回線装置又は通信回線を有する情報システム。以下この項において同じ。)については、システムが保有する情報の格付けに従って、サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

サーバ装置、端末及び通信回線装置について、以下【推奨事項】を例とするサービス不能攻撃に対抗するための機能を設けている場合は、これらを有効にしてサービス不能攻撃に対処すること。

【推奨事項】

- パケットフィルタリング
- 3-way handshake 時のタイムアウトの短縮
- 各種 Flood 攻撃への防御
- アプリケーションゲートウェイ機能

各対策の解説については、「6. 4 サービス不能攻撃対策」を参照のこと

(d) 標的型攻撃対策

【主旨・目的】

標的型攻撃とは、特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入

念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃である。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。

したがって、標的型攻撃による組織内部への侵入を低減する対策（入口対策）、並びに内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）からなる、多重防御の情報セキュリティ対策体系によって、標的型攻撃に備える必要がある。

【対策項目】

①入口対策

情報セキュリティ責任者は、サーバ装置及び端末について、組織内部への侵入を低減するため、以下【推奨事項】を例とする対策（入口対策）を講ずること。

②内部対策

情報セキュリティ責任者は、サーバ装置及び端末について、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される、認証サーバやファイルサーバ等の重要なサーバについては、以下【推奨事項】を例とする対策を行うこと。

【推奨事項】

＜①に関する推奨事項＞
- 不要なサービスについて機能を削除又は停止する。
- 不審なプログラムが実行されないよう設定する。
- パーソナルファイアウォール等を用いて、サーバ装置及び端末に入力される通信及び出力される通信を必要最小限に制限する。

＜②に関する推奨事項＞
- 重要サーバについては、組織内ネットワークを複数セグメントに区切った上で、重要サーバ類専用のセグメントに設置し、他のセグメントからのアクセスを必要最小限に限定する。また、インターネットに直接接続しない。
- 不要な管理者権限アカウントを削除する。
- 管理者権限アカウントのパスワードは、容易に推測できないものに設定する。

（e）パスワードリスト攻撃対策

【主旨・目的】

パスワードリスト攻撃とは、攻撃者が何らかの方法で事前に入手した ID とパスワードのリストを使用し、ログイン機能を持つインターネットサービスに不正にログインを試みる攻撃手法である。もし重要インフラ利用者が ID とパスワードを他のインターネットサービス等で使い回していると、第三者による

なりすましログインを可能にしてしまい、顧客情報の不正操作や情報流出のリスクがある。

鉄道分野では、顧客向けのインターネットサービス（座席予約等）を提供している事業者が想定されるため、パスワードリスト攻撃への対策が必要である。

【対策項目】

情報セキュリティ責任者は、顧客向けに提供するインターネットサービスには、以下【推奨事項】を例とする対策を講ずること。

【推奨事項】

- 多要素認証機能（認証コード、ワンタイムパスワード等）の実装
- アカウントロック機能の実装
- 不正ログイン試行を検知する機能（通常とは異なる IP アドレスからのアクセス時にメールで通知等）の実装
- ログイン履歴表示機能の実装

多要素認証機能の解説については、「6.5 多要素認証機能」参照のこと

（3） 情報システム施設に係る入退出管理（物理的な不正侵入の防止）

【主旨・目的】

サーバ装置、端末等が、不特定多数の者により物理的に接触できる設置環境にある場合においては、悪意ある者によるなりすまし、物理的な装置の破壊のほか、サーバ装置や端末の不正な持ち出しによる情報の漏えい等のおそれがある。その他、設置環境に関する脅威として、災害の発生による情報システムの損傷等もある。

したがって、執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保し、当該区域で取り扱う情報や情報システムのセキュリティを確保する必要がある。

【対策項目】

①立入り及び退出の管理

情報セキュリティ責任者は、情報処理設備を含む領域を保護するために、セキュリティ境界を明確に定め、適切な入退管理策によってセキュリティの保たれた領域（以下、要管理対策区域）とすること。また、要管理対策区域への全ての者の入退出を記録・管理し、立入りは業務上必要な者に限定するとともに、その立入りに際しては、本人認証や責任者による事前承認などの管理を実施すること。立入りを許可された者については随時見直し、入室が不要となった者については、速やかに登録許可を解除すること。

②訪問者及び受渡業者の管理

情報セキュリティ責任者は、要管理対策区域への訪問者がある場合には、訪問者の氏名、所属及び訪問目的並びに訪問相手の氏名及び所属の提示を求め、立入りを審査するための手続を整備

すること。
また、要管理対策区域内において、訪問者と継続的に立入りが許可された者とを外見上判断できる措置を講じ、必要に応じて取扱者が訪問者に付き添うための措置を講ずること。

訪問者への具体的な情報セキュリティ対策としては、以下【推奨事項】の対策を講ずることが望ましい。

③要管理対策区域内のセキュリティ管理
情報セキュリティ責任者は、要管理対策区域内のセキュリティを強化するために、その領域に設置された情報資産の重要性に応じて、必要かつ適切な措置を講ずること。

要管理対策区域内のセキュリティ強化策としては、以下【推奨事項】の対策を講ずることが望ましい。

④脅威に応じた物理的対策
情報セキュリティ責任者は、情報システムについては、システムが保有する情報の格付けに従って、自然災害、サイバー攻撃、IT 障害等の様々な脅威からサーバ装置、端末及び通信回線装置を保護するための物理的な対策を検討すること。

物理的対策としては、以下【推奨事項】の対策を講ずることが望ましい。

【推奨事項】

＜②に関する推奨事項＞
・ 取扱者は、身分証明書等を着用、明示すること
・ 訪問者に入館カード等を貸与し、着用、明示させること
・ 訪問者と継続的に立入りを許可された者に貸与する入館カード等やそれと併せて貸与するストラップ等の色分けを行うこと
・ 訪問者に貸与した入館カード等は、悪用防止のため退出時に回収すること
・ 訪問者が不正な行為を行うことを防止するために、作業を行う場合は立会いや監視カメラ等により監視を行うこと
＜③に関する推奨事項＞
・ 要管理対策区域の存在又はそこでの作業は、その必要がある要員だけが知っているようにすること
・ 取扱者は、要管理対策区域内において、身分証明書を他の取扱者から常時視認することが可能な状態にすること
・ 付添いを伴わない見知らぬ人及び目に見える身分証明を着用していない人に対しては、誰であるか問い掛けるよう奨励すること
・ 本人認証や責任者による事前承認などの管理を充実すること
・ 許可されていない者の入室手続きを定めること
・ 要管理対策区域内での作業を監視するための措置を講ずること
・ 情報システムに関連しない機器（私物のスマートフォン、モバイル端末、デジタルカメラ等の撮影機器、IC レコーダー等の録音機器、USB メモリ等の外部電磁的記録媒体等が含まれる）の要管

理対策区域への持込みについて制限すること
・ 情報システムに関連する機器の要管理対策区域への持込み及び要管理対策区域からの持出には、情報セキュリティ責任者の承認を求めること
・ 情報システムに関連する機器の不正な持ち出しが行われていないかを確認するために定期的又は不定期に施設からの退出時に持ち物検査を行うこと
＜④に関する推奨事項＞
・ 免震・耐震設備を有する施設、免震機能を有したサーバラック、人体・通信装置・環境に対する安全性を考慮した消火設備、無停電電源装置等の非常電源装置等の設置を検討すること
・ すべての外部扉及びアクセス可能な窓を防御し、侵入者の検知システムを設置すること
・ 建物は目立たせず、その用途を示す表示は最小限とすること
・ 緊急時に用いる代替装置及びバックアップされた媒体は、主事業所から十分に離れた場所に置くこと

4.1.5.2 情報セキュリティ対策に係る設計・実装・保守

【対策の指針】

技術については、情報セキュリティ要件に応じて情報システムへの情報セキュリティ対策を実装する。その際、情報セキュリティ対策機能の実装が業務要件にて要するシステム性能を損なわないよう留意が必要である。また、ノウハウの蓄積を考慮し、情報セキュリティ対策の実装に係る設計資料を作成する。

運用については、情報セキュリティ要件に応じて情報セキュリティ対策を実装した情報システムの運用設計・手順書化を経て、安定した運用を実現する。また、情報セキュリティ対策の有効性を維持するため、認証に要するユーザー登録等の保守をもれなく行う。

(1) 情報システムのセキュリティ要件

【主旨・目的】

情報システムは、目的業務を円滑に遂行するため、その企画・要件定義、構築、運用・保守、更改・廃棄及び見直しのライフサイクルを通じて様々な要件を満たすことが必要である。その要件の中には情報セキュリティの観点からの要件も含まれ、情報システムのライフサイクルにあわせて情報セキュリティ対策を実施する必要がある。

【対策項目】

①情報システム企画・要件定義

情報セキュリティ責任者は、情報システムについて、ライフサイクル全般にわたってセキュリティ維持が可能な体制の確保を、情報システムを統括する責任者に求めること。

情報セキュリティ責任者は、情報システムのセキュリティ要件を決定し、セキュリティ要件を満たすために、機器等の購入(購入に準ずるリースを含む。)及び情報システム開発において必要な対策、機器等の選定基準、情報セキュリティについての機能の設定、情報セキュリティについての脅威への対策、並びに情報システムの構成要素についての対策について定めること。

情報セキュリティ責任者は、情報システムの取扱いに関し、取扱者が理解・遵守するために周知に努め、教育・訓練その他必要な措置を実施すること。

情報システムの企画・要件定義時には、以下【推奨事項】に示す情報セキュリティ対策を講ずることが望ましい。

②情報システムの構築

情報セキュリティ責任者は、情報システムの構築に際しては、情報セキュリティの観点から必要な措置を講ずること。

情報システムの構築時には、以下【推奨事項】に示す情報セキュリティ対策を講ずることが望ましい。

【推奨事項】

＜①に関する推奨事項＞
- 情報セキュリティ責任者は、開発する情報システムが運用される際に関連する情報資産に対して想定されるセキュリティ脅威の分析結果、及び当該情報システムにおいて取り扱う情報の格付けに応じて、セキュリティ機能（主体認証、アクセス制御、権限管理、ログ管理、暗号化機能等）要件を適切に策定し、仕様書等に明確に記述すること
- 情報セキュリティ責任者は、開発する情報システムが運用される際に利用されるセキュリティ機能についての管理機能要件を適切に策定し、仕様書等に明確に記述すること
- 情報セキュリティ責任者は、開発する情報システムで利用するソフトウェアについて、当該保守期限を考慮するなどして、当該情報システムの次期更改時期まで対策用ファイルの提供が継続されると見込まれるソフトウェアを選定すること。また、適宜入手した保守期限の情報から必要と判断した場合は、後継となるソフトウェアへの更新等の計画を策定すること。
- 情報セキュリティ責任者は、情報システムの設計について、その情報セキュリティに関する妥当性を確認するための設計レビューの範囲及び方法を定め、これに基づいて設計レビューを実施すること
- 情報セキュリティ責任者は、開発する情報システムに関連する脆弱性についての対策（情報システムにおいて処理するデータ及び入出力されるデータの情報セキュリティに関する妥当性を確認する機能等）を仕様書等に明確に記述すること
- 情報セキュリティ責任者は、開発する情報システムに適切なセキュリティ要件が策定されていることを第三者が客観的に確認する必要がある場合には、これを実現するセキュリティ機能の設計について第三者機関によるセキュリティ設計仕様書（ST：Security Target）の ST 評価・ST 確認を受けること

＜②に関する推奨事項＞
- セキュリティ要件に基づき定めた情報セキュリティ対策を行うこと
- 構築した情報システムを運用保守段階へ移行するに当たり、移行手順及び移行環境に関して、情報セキュリティの観点から必要な措置を講ずること
- 機器等の納入時又は情報システムの受入れ時の確認・検査において、仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認すること

（2）端末、サーバ装置、複合機及び特定用途機器

（a）端末

【主旨・目的】

端末の利用に当たっては、当該端末を利用する者が専門的知識を有していない場合が多いことから、当該端末を利用する者の不適切な利用や過失等による不正プログラム感染等のリスクが高い。ま

た、モバイル端末については、紛失又は盗難のリスクも高くなることから、適切な対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、端末で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

情報セキュリティ責任者は、端末の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

情報セキュリティ責任者は、事業者外へ持ち出すモバイル端末について、盗難等の際に第三者により情報窃取されることを防止するための対策を講ずること。

(b) サーバ装置

【主旨・目的】

サーバ装置については、当該サーバ装置の内蔵記録媒体等に大量の情報を保存している場合が多いことから、当該情報の漏えい又は改ざんによる影響も端末と比較して大きなものとなる。また、サーバ装置は、通信回線等を介してその機能が利用される場合が多く、不正プログラム感染や不正侵入等を受けるリスクが高い。事業者が有するサーバ装置が不正アクセスや迷惑メール送信の中継地点に利用されるようなことになれば、顧客からの信頼を大きく損なうことにもなる。さらに、サーバ装置は、同時に多くの者が利用できるため、その機能が停止した場合に与える影響が大きいことから、適切な対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、サーバ装置の盗難、不正な持ち出し、第三者による不正操作、表示用デバイスの盗み見等の物理的な脅威から保護するための対策を講ずること。

情報セキュリティ責任者は、障害や過度のアクセス等によりサービスが提供できない事態となることを防ぐため、将来の見通しも考慮し、サービス提供に必要なサーバ装置を冗長構成にするなどにより可用性を確保すること。

情報セキュリティ責任者は、サーバ装置で利用を認めるソフトウェア及び利用を禁止するソフトウェアを定めること。

情報セキュリティ責任者は、通信回線を経由してサーバ装置の保守作業を行う場合は、送受信される情報を暗号化する等情報が漏えいすることを防止するための対策を講ずること。

情報セキュリティ責任者は、システム運用に不要なサーバアプリケーションについては、機能を無効化して稼動させること。

(c) 複合機及び特定用途機器

【主旨・目的】

複合機（プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器）は、事業者内通信回線や公衆電話網等の通信回線に接続して利用されることが多く、その場合

には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定される。

また、事業者においては、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システムが利用されている。これらの情報システムにおいては、汎用的な機器のほか、システム特有の特定用途機器が利用されることがあり、特定用途機器についても、当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により脅威が存在する場合がある。

したがって、複合機や特定用途機器に関しても情報システムの構成要素と捉え、責任者を明確にして対策を講ずることが重要である。

【対策項目】

①複合機

情報セキュリティ責任者は、複合機を調達する際には、当該複合機が備える機能、設置環境並びに取り扱う情報の格付及び取扱制限に応じ、適切なセキュリティ要件を策定すること。

情報セキュリティ責任者は、以下【推奨事項】を例とする運用中の複合機に対する、IT 障害への対策を講ずること。

②特定用途機器

情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により脅威が存在する場合には、当該機器の特性に応じて、以下【推奨事項】を例とする対策を講ずること。

【推奨事項】

＜①に関する推奨事項＞
- 複合機について、利用環境に応じた適切なセキュリティ設定を実施する。
- 複合機が備える機能のうち利用しない機能を停止する。
- 印刷された書面からの情報の漏えいが想定される場合には、複合機が備える操作パネルで認証が成功した者のみ印刷が許可される機能等を活用する。
- 事業者内通信回線とファクシミリ等に使用する公衆通信回線が、複合機の内部において接続されないようにする。
- 複合機をインターネットに直接接続しない。
- リモートメンテナンス等の目的で複合機がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
- 複合機を利用する者ごとに許可される操作を適切に設定する。

＜②に関する推奨事項＞
- 特定用途機器について、利用環境に応じた適切なセキュリティ設定を実施する。
- 特定用途機器が備える機能のうち利用しない機能を停止する。
- 特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
- インターネットに接続されている特定用途機器についてソフトウェアに関する脆弱性が存在しないか確認し、脆弱性が存在する場合、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。

(3) アプリケーションソフトウェア

(a) 電子メール

【主旨・目的】

電子メールの送受信とは情報のやり取りにほかならないため、不適切な利用により情報が漏えいする等の機密性に対するリスクがある。また、電子メールサーバに過負荷等が加えられることによって、機能が損なわれる等の可用性に対するリスクがある。この他、悪意ある第三者等によるなりすまし等に電子メールを利用する従事員が巻き込まれるリスクもある。このようなリスクを回避するためには、適切な電子メールサーバの管理及び電子メールの利用が必要であり、電子メールサーバの管理及び電子メールの利用に関する対策基準を定める必要がある。

【対策項目】

情報セキュリティ責任者は、電子メールにおける情報セキュリティ上のリスクを軽減するための管理策の必要性について検討すること。

電子メール導入については、以下の対策について考慮することが望ましい。

【推奨事項】

- 添付ファイルの保護
- 不正中継禁止
- 送受信容量の制限
- 自動転送の制限
- 業務外利用の禁止
- 送信先アドレス漏えいの防止
- 電子署名機能の導入
- 安全性が客観的に評価された暗号技術の利用
- 迷惑メールフィルターの導入
- 電子メール送信時及び受信時の送信ドメイン認証(SPF等)の導入

(b) ウェブ

【主旨・目的】

インターネット上に公開するウェブサーバは、常に攻撃を受けるリスクを抱えている。様々な攻撃により、ウェブコンテンツ(ウェブページとして公開している情報)が改ざんされたり、ウェブサーバが利用不能にされたり、又はウェブサーバが侵入されるなどの被害が想定されるため、適切な対策を組み合わせて実施することが求められる。

【対策項目】

情報セキュリティ責任者は、ウェブサーバを用いて提供するサービスにおいて、システムが保有する情報の格付けに応じて、想定される脅威から保護すべき情報を特定し、対策を行う必要性の有無を検討し、適切な対策を講ずること。

ウェブ導入時の対策としては、以下の対策を講ずることが望ましい。

【推奨事項】

・ 情報セキュリティ責任者は、ウェブアプリケーションの開発において、以下に示すような既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること
  a) SQL インジェクション脆弱性
  b) OS コマンドインジェクション脆弱性
  c) ディレクトリトラバーサル脆弱性
  d) セッション管理の脆弱性
  e) アクセス制御欠如と認可処理欠如の脆弱性
  f) クロスサイトスクリプティング脆弱性
  g) クロスサイトリクエストフォージェリ脆弱性
  h) クリックジャッキング脆弱性
  i) メールヘッダインジェクション脆弱性
  j) HTTP ヘッダインジェクション脆弱性
  k) eval インジェクション脆弱性
  l) レースコンディション脆弱性
  m) バッファオーバーフロー及び整数オーバーフロー脆弱性
  各脆弱性の解説については、「6. 6 ウェブアプリケーションの脆弱性」を参照のこと
・ 情報セキュリティ責任者は、ウェブサーバを用いて提供するサービスにおいて、システムが保有する情報の格付けに応じて、通信の盗聴から保護すべき情報を特定し、暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること
・ 情報セキュリティ責任者は、ウェブサーバの正当性を保証するために電子証明書を利用すること

(4) 通信回線及び通信回線装置

(a) 通信回線共通対策

【主旨・目的】

通信回線の利用については、当該通信回線の不正利用、これに接続されたサーバ装置、端末又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、通信事業者の公衆回線や事業者専用の通信回線の運用主体又は有線回線や無線 LAN 回線等の物理的な回線の種類によって情報セキュリティリスクが異なることを十分考慮し、対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、通信回線構築・運用に係るリスクに対応するため、通信回線におけるセキュリティを実現・維持するために、適切な対策を講ずること。

情報セキュリティ責任者は、通信回線に論理的に接続する際の審査手続を整備し、承認を受けていない者からの通信を遮断するための対策を講ずること。

情報セキュリティ責任者は、通信回線の情報セキュリティ維持に関する対策として、アクセス制御、経路制御、送受信情報の暗号化、及び物理的セキュリティなどの必要性の有無を検討し、適切な対

策を講ずること。

通信回線の構築時には、以下の対策を講ずることが望ましい。

【推奨事項】

- 情報セキュリティ責任者は、通信回線構築によるリスクを検討し、通信回線を構築すること
- 情報セキュリティ責任者は、通信回線に接続されるサーバ装置、端末をグループ化し、それぞれ通信回線上で分離すること
- 情報セキュリティ責任者は、グループ化されたサーバ装置及び端末間での通信要件を検討し、当該通信要件に従って通信回線装置を利用しアクセス制御及び経路制御を行うこと
- 情報セキュリティ責任者は、通信する情報の格付けに従って、通信回線を用いて送受信される情報の暗号化を行う必要性の有無を検討し、必要があると認めたときは、情報を暗号化すること
- 情報セキュリティ責任者は、通信する情報の格付けに従って、通信回線に利用する物理的な回線のセキュリティを検討し、必要な対策を講ずること
- 情報セキュリティ責任者は、取扱者が通信回線へ情報システムを接続する際に、当該情報システムが接続を許可されたものであることを確認するための措置を講ずること
- 情報セキュリティ責任者は、遠隔地から通信回線装置に対して、保守又は診断のために利用するサービスによる接続について情報セキュリティを確保すること
- 情報セキュリティ責任者は、通信回線装置に存在する公開された脆弱性から通信回線装置を保護するための対策を講ずること
- 情報セキュリティ責任者は、通信回線装置を要管理対策区域に設置すること
- 情報セキュリティ責任者は、電気通信事業者の通信回線サービスを利用する場合には、情報セキュリティ水準及びサービスレベルを含む事項に関して契約時に取り決めておくこと
- 情報セキュリティ責任者は、事業者内通信回線にインターネット回線、公衆通信回線等の事業者外通信回線を接続する場合には、事業者内通信回線及び当該事業者内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること
- 情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアを定め、ソフトウェアを変更する際の許可申請手順を整備すること

(b) リモートアクセス環境導入時の対策

【主旨・目的】

リモートアクセス環境の利用については、当該通信回線の不正利用、これに接続されたサーバ装置、端末又は通信回線装置への不正アクセス、送受信される情報の盗聴、改ざん及び破壊等、当該通信回線を含む情報システム及び当該情報システムが取り扱う情報の情報セキュリティが損なわれるおそれを有している。また、利用する回線により想定される脅威及びリスクが異なる。これらのことを踏まえ、リモートアクセス環境導入に関する対策基準を定める必要がある。

【対策項目】

①VPN 回線利用時の対策

情報セキュリティ責任者は、VPN 環境を整備してリモートアクセス環境を構築する場合には、以下【推奨事項】に挙げる事項を含む対策を講ずることが望ましい。

②公衆電話網利用時の対策

情報セキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合には、以下【推奨事項】に挙げる事項を含む対策を講ずることが望ましい。

【推奨事項】

＜①に関する推奨事項＞
・ 利用開始及び利用停止時の申請手続の整備
・ 通信内容の暗号化
・ 通信を行う端末の識別又は認証
・ リモートアクセス環境を利用する者の認証
・ 主体認証ログの取得及び管理
・ リモートアクセスにおいて利用可能な通信回線の範囲の制限
・ アクセス可能な情報システムの制限
・ リモートアクセス中の他の通信回線との接続禁止
＜②に関する推奨事項＞
・ 利用開始及び利用停止時の申請手続の整備
・ 通信を行う者又は発信者番号による識別及び主体認証
・ 主体認証ログの取得及び管理
・ リモートアクセス経由でアクセスすることが可能な情報システムの制限
・ リモートアクセス中に他の通信回線との接続の禁止

（c）無線 LAN 環境導入時の対策

【主旨・目的】

無線 LAN 技術を利用して事業者内通信回線を構築する場合は、通信回線共通対策に加えて、通信内容の秘匿性を確保するために通信路の暗号化を行った上で、その他の情報セキュリティ確保のために必要な措置を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、無線 LAN 環境を構築する場合には、以下に挙げる事項を含む対策を講ずることが望ましい。

【推奨事項】

・ 利用開始及び利用停止時の申請手続の整備
・ 通信内容の暗号化
・ 通信を行う端末の識別又は認証
・ 無線 LAN を利用する者の認証
・ 主体認証ログの取得及び管理
・ 無線 LAN 経由でアクセス可能な情報システムの明確化
・ 無線 LAN に接続する端末及び通信回線装置の管理
・ 不正プログラム感染を認知した場合の対処手順

4.2 「Do（実働）」の観点

4.2.1 「平時・障害発生時共通」の観点

4.2.1.1 情報セキュリティ対策の運用（監視・統括）

【対策の指針】

構築した情報セキュリティ対策の運用状況については、定期的に情報セキュリティ責任者が把握していることを常態化する。

（1） 情報システムの運用

【主旨・目的】

情報システムの運用・保守においては、情報システムに実装されたセキュリティ機能が適切に運用されなければ、情報システムに係る様々な情報セキュリティ脅威に対抗できない。また、更改・廃棄においては、情報システムに残存する情報の漏えい等のリスクがある。そのため、情報システムの運用・保守、更改・廃棄、見直しにおいては、ライフサイクルに応じた適切な措置を実施する必要がある。

【対策項目】

①情報システムの運用・保守

情報セキュリティ責任者は、情報システムの運用・保守に際しては、情報システムに実装されたセキュリティ機能を適切に運用すること。

また、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること

②情報システムの更改・廃棄

情報セキュリティ責任者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、移行作業における情報セキュリティ対策及び不要な情報の抹消を適切に実施すること。

③情報システムについての対策の見直し

情報セキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

（2） 情報システムの構成要素の運用

【主旨・目的】

端末、サーバ装置、通信回線・通信回線装置、複合機及び特定用途機器のような情報システムの構成要素は、それぞれ保持する情報や使われ方等性質が異なるため、運用においては構成要素個別の情報セキュリティ対策を実施する必要がある。

【対策項目】

① 端末の運用時・運用終了時

情報セキュリティ責任者は、利用を認めるソフトウェア及び利用を禁止するソフトウェアについて定期的に見直しを行うこと。

情報セキュリティ責任者は、主管する範囲の端末で利用されている全てのソフトウェアの状態を定期的に調査し、不適切な状態にある端末を検出等した場合には、改善を図ること。

情報セキュリティ責任者は、端末の運用を終了する際に、端末の電磁的記録媒体の全ての情報を抹消すること。

端末を利用する取扱者は、端末が取り扱う情報の格付け及び利用方法に応じて、以下【推奨事項】に示す情報セキュリティ対策を実施することが望ましい。

②サーバ装置の運用時・運用終了時

情報セキュリティ責任者は、サーバ装置について、構成管理・変更管理を実施すること。
また、サーバ装置の運用管理について、作業日、作業を行ったサーバ装置、作業内容及び作業者を含む事項を記録すること。

情報セキュリティ責任者は、サーバ装置に保存されている情報について、情報の格付けに従って、定期的にバックアップを取得すること。また、取得した情報を記録した媒体について、安全管理措置を講ずること。

情報セキュリティ責任者は、サーバ装置のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、不正行為及び不正利用を含むトラブル事象の発生を検知するための措置を講ずること。

情報セキュリティ責任者は、サーバ装置の運用を終了する際に、サーバ装置の電磁的記録媒体の全ての情報を抹消すること。

③通信回線及び通信回線装置の運用時・運用終了時

情報セキュリティ責任者は、通信回線及び回線装置について、構成管理・変更管理を実施すること。

情報セキュリティ責任者は、通信回線及び回線装置の運用管理について、作業日、作業を行った通信回線・回線装置、作業内容及び作業者を含む事項を記録すること。

情報セキュリティ責任者は、経路制御及びアクセス制御を適切に運用し、通信回線や通信要件の変更の際及び定期的に、経路制御及びアクセス制御の設定の見直しを行うこと。

情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある通信回線装置を認識した場合には、改善を図ること。

情報セキュリティ責任者は、日常的に、通信回線の通信内容、通信回線及び回線装置のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、通信回線の性能低下、不正行為及び不正利用を含むトラブル事象の発生を推測又は検知するための措置を講ずること。

情報セキュリティ責任者は、通信回線装置の利用を終了する場合には、通信回線装置の電磁的記録媒体のすべての情報を復元できない状態にすること。

④複合機及び特定用途機器の運用時・運用終了時

情報セキュリティ責任者は、特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視すること。

情報セキュリティ責任者は、複合機及び特定用途機器について、構成管理・変更管理を実施すること。

情報セキュリティ責任者は、複合機及び特定用途機器の運用管理について、作業日、作業を行った複合機及び特定用途機器、作業内容及び作業者を含む事項を記録すること。

情報セキュリティ責任者は、複合機及び特定用途機器が動作するために必要なソフトウェアの状態を定期的に調査し、許可されていないソフトウェアがインストールされているなど、不適切な状態にある複合機及び特定用途機器を認識した場合には、改善を図ること。

情報セキュリティ責任者は、複合機及び特定用途機器のセキュリティ状態、負荷状況などのシステムの稼動状況を監視し、不正行為及び不正利用を含むトラブル事象の発生を検知するための措置を講ずること。

情報セキュリティ責任者は、内蔵電磁的記録媒体の全領域完全消去機能（上書き消去機能）を備える複合機及び特定用途機器については、当該機能を活用することにより複合機及び特定用途機器内部の情報を抹消すること。当該機能を備えていない複合機及び特定用途機器については、外部委託先との契約時に外部委託先に複合機及び特定用途機器内部に保存されている情報の漏えいが生じないための対策を講じさせることを、契約内容に含むようにするなどの別の手段で対策を講ずること。

【推奨事項】

＜①に関する推奨事項＞

- 取扱者は、業務の遂行以外の目的で情報システムを利用しないこと。
- 取扱者は、情報セキュリティ責任者が接続許可を与えた通信回線以外に端末を接続しないこと。
- 取扱者は、事業者内通信回線に、情報セキュリティ責任者の接続許可を受けていない端末を接続しないこと。
- 取扱者は、端末で利用を禁止するソフトウェアを利用しないこと。また、端末で利用を認めるソフトウェア以外のソフトウェアを業務上の必要により利用する場合は、情報セキュリティ責任者の承認を得ること。
- 取扱者は、端末の設置場所から離れる場合等、第三者による不正操作のおそれがある場合は、端末を不正操作から保護するための措置を講ずること。
- 取扱者は、端末を事業者外に持ち出す場合には、情報セキュリティ責任者の許可を得ること。

4.2.1.2 情報セキュリティ対策の運用状況把握

【対策の指針】

経営層は、情報セキュリティ対策の運用状況について、把握する。

【主旨・目的】

情報セキュリティ対策は、事業継続を念頭に置いた全社的なリスクマネジメントの一部であることを

踏まえ、リスクマネジメントと情報セキュリティ対策が整合する取組となるように留意する。これらが整合するよう情報セキュリティ対策を経営層が担う全社的なリスクマネジメントの一部と位置付けるとともに、担当者のみならず経営層も関与した全社的な体制の下で情報セキュリティ対策に取り組む必要がある。

【対策項目】

情報セキュリティ責任者は、情報セキュリティ対策の運用状況を定期的に経営層に報告すること。

4.2.2 「平時」の観点

4.2.2.1 情報セキュリティ対策の運用

【対策の指針】

情報システムの運用状況が平時の状況やしきい値と比して異なる状況にあること等を検知し、予兆を把握する。

また、システム保守において、組織やシステムユーザーの変更、システムのチューニング等といった登録値の変更等を通じて、情報セキュリティ対策の水準を維持する。

加えて、情報セキュリティに係る教育を全社的に行う。

(1) 情報システムの運用・保守

【主旨・目的】

IT 障害発生時に迅速に対応するためには、情報システムの運用状況が平時の状況やしきい値と比して異なる状況にあること等を検知し、IT 障害の予兆を把握することが重要である。また、システム保守において、組織やシステムユーザーの変更、システムのチューニング等といった登録値の変更等を通じて、情報セキュリティ対策の水準を維持する必要がある。

【対策項目】

①ソフトウェアに関する脆弱性対策

情報セキュリティ責任者は、情報システム上で利用するソフトウェアに関連する脆弱性情報の収集に努め、当該情報から情報システムのリスクを分析した上で、脆弱性ごとに対策計画を作成し、適切な対策を講ずること。

ソフトウェアに関する脆弱性対策計画を作成にあたっては、以下【推奨事項】について判断することが望ましい。

②不正プログラム対策

情報セキュリティ責任者は、不正プログラムに関する情報の収集に努め、当該情報について対処の要否を決定し、特段の対処が必要な場合には、取扱者にその対処の実施に関する指示を行うこと。

情報システムの運用時における不正プログラム対策としては、以下【推奨事項】の対策を講ずることが望ましい。

③サービス不能攻撃対策

情報セキュリティ責任者は、サービス不能攻撃対策を講じた情報システムについては、監視方法及び監視記録の保管期間を定め、サーバ装置、端末、通信回線装置及び通信回線を監視し、その記録を保存すること。

④パスワードリスト攻撃対策

情報セキュリティ責任者は、重要インフラ利用者に ID・パスワードの使い回しをしないなどの注意喚起を行うこと。

情報セキュリティ責任者は、認証ログを監視し、不正ログイン試行を検知した場合、当該 IP アドレスからの通信を遮断する等の対応を検討すること。

情報セキュリティ責任者は、長期間利用されていないアカウントについて、停止・削除する等の対応を検討すること。

⑤電子メール運用時の対策

取扱者は、電子メール利用時には、以下【推奨事項】の対策を講ずること。

⑥ウェブ運用時の対策

取扱者は、ウェブクライアントが動作するサーバ装置又は端末にソフトウェアをダウンロードする場合には、電子署名により当該ソフトウェアの配布元を確認すること。

【推奨事項】

＜①に関する推奨事項＞
- 対策の必要性
- 対策方法
- 対策方法が存在しない場合の一時的な回避方法
- 対策方法又は回避方法が情報システムに与える影響
- 対策の実施予定
- 対策テストの必要性
- 対策テストの方法
- 対策テストの実施予定

＜②に関する推奨事項＞
- 取扱者は、不正プログラム対策ソフトウェア等により不正プログラムとして検知される実行ファイルを実行せず、データファイルをアプリケーション等で読み込まないこと
- 取扱者は、不正プログラム対策ソフトウェア等にかかわるアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること
- 取扱者は、不正プログラム対策ソフトウェア等による不正プログラムの自動検査機能を有効にすること
- 取扱者は、不正プログラム対策ソフトウェア等により定期的にすべての電子ファイルに対して、不正プログラムの有無を確認すること

・ 取扱者は、外部からデータやソフトウェアをサーバ装置及び端末等に取り込む場合又は外部にデータやソフトウェアを提供する場合には、不正プログラム感染の有無を確認すること
・ 取扱者は、ソフトウェアのセキュリティ機能を活用し、不正プログラム感染の予防に努めること
＜⑤に関する推奨事項＞
・ 送信者のメールアドレス、件名、本文に不審な点が無いか、総合的に判断する。
・ 不審な形式の添付ファイル（.exe、.bat、心当たりのない拡張子 等）を開かない。
・ 文書ファイルが添付されていても、業務上不要と考えられる添付ファイルは開かない。
・ メールに記載されたURLリンクに安易にアクセスしない。

（2） 情報セキュリティの教育

【主旨・目的】

事業者内規程が適切に整備されているとしても、その内容が取扱者に周知されず、これが遵守されない場合には、情報セキュリティ水準の向上を望むことはできない。このため、全ての取扱者が、情報セキュリティの教育を通じ、規程への理解を深め、情報セキュリティ対策を適切に実施することが必要である。

【対策項目】

情報セキュリティ責任者は、情報セキュリティ教育の計画に従い、セキュリティ要求事項、法律上の責任及び業務上の管理策とともに、情報又はサービスへのアクセスを許可する前に実施すること。

4.2.2.2 情報セキュリティ対策状況の対外説明

（1） IT障害防止のための取組みに関する情報の提供

（a） 重要インフラ事業者間の情報共有

重要インフラ事業者は、所属するセプターにおいて、相互にIT障害やサイバー攻撃に係る情報、復旧手法情報、早期警戒情報等の共有を行うこと。また、必要に応じて、他分野の重要インフラ事業者との情報共有にセプターカウンシルを活用すること。

重要インフラ事業者は、必要に応じてIT障害やサイバー攻撃に係る情報連絡を国土交通省に行う。なお、犯罪被害にあった場合は、自主的な判断により事案対処省庁に通報を行う。

（b） 重要インフラ事業者外への情報共有

重要システムの停止・低下を防止するための情報セキュリティ対策に関する取組みについて重要インフラ利用者が安心できるよう提供範囲に留意しつつ、可能な範囲（情報セキュリティ報告書、CSR報告書、各種ディスクロージャ資料等）で情報提供するよう努めること。

4.2.3 「障害発生時」の観点

4.2.3.1 IT障害に対する防護・回復

【対策の指針】

策定したIT-BCPを発動し、規定に沿った業務継続を進めるとともに、早期復旧に向けた対応を行

う。その際、原因究明等に必要なログ等の電子的記録を収集・分析し、IT障害をもたらした原因への適切な対処を可能とする。

(1) 本社等重要拠点の機能の確保

【主旨・目的】

緊急事態時には、本社等の重要拠点が被災した場合に備え、重要拠点の機能を確保し、重要業務を継続するための、対策を検討する必要がある。

【対策項目】

情報セキュリティ責任者は、緊急事態時における対策を検討・指揮するため、緊急時対策の責任者及び幹部社員等が集合する場所を確保すること。また、本社、あるいは支店、支社などの重要な拠点が被災した場合に備え、集合場所と、継続を優先する業務を規定すること。

本社等の重要拠点の機能の確保に関し、事業継続計画を検討する際には、以下の点を考慮することが望ましい。

【推奨事項】

- 被災地での業務の再開以外に、非被災地での業務の継続も検討すること。(例えば、被災地以外の拠点に指揮命令権を移すなど)なお、被災地以外に拠点を移すことの検討は必須ではないが、その検討をせずに利害関係者の理解が得られるかを慎重に考慮する必要がある
- 遠隔地の文書・電子データ保存サービスの活用すること
- 時差を考慮すること(日本が休日・夜間であっても海外は営業時間であることもあるため海外への情報発信が必要)
- 自治体等の各種制度や防災隣組の機能など、地域の資源を活用すること

(2) 対外的な情報発信及び情報共有

【主旨・目的】

緊急事態発生後は、事業者活動が関係者から見えなくなる、何をしているのか全然わからないといった、いわゆるブラックアウトを防ぐための対策を講ずる必要がある。

【対策項目】

情報セキュリティ責任者は、緊急事態発生後に、取引先、顧客、取扱者、株主、地域住民、政府・自治体などと情報を共有するために、4.1.4.1(3)(b)で定める必要な対策を講ずること。

(3) 情報システムのバックアップ

【主旨・目的】

情報システムは事業を支える重要なインフラとなっており、緊急事態発生時には、通常業務に必要なデータの欠落や不整合による障害が発生するおそれがある。これらを防ぐとともに早期復旧を図るため、あらかじめ策定した計画に基づいたバックアップ運用を実施する必要がある。

【対策項目】

情報セキュリティ責任者は、4.1.2.2(2)で策定した計画に基づき、必要な情報のバックアップを取得し、同じ IT 障害で同時に被災しない場所に保存すること。

4.2.3.2 情報セキュリティ対策状況の対外説明

【対策の指針】

IT障害の状況や復旧等の情報提供については、策定したIT-BCPに沿って、情報に基づく対応の5W1H の理解の下、サービスの利用者への情報提供等、他の関係主体との連携統制の取れた対応を行う。

(1) IT 障害による重要インフラサービスの停止等の情報の提供

重要システムの停止・低下により、旅客の輸送に支障を及ぼす列車の遅延や運休が発生した際、重要インフラ利用者が安心して対応が行えるよう情報提供を行うこと。

4.3 「Check(確認)・Act(是正)」の観点

4.3.1 「平時」の観点

【対策の指針】

情報セキュリティ対策の運用、内部監査・外部監査、ITに係る環境変化の調査・分析結果及び演習・訓練を通じた課題抽出として、それぞれの取組の中で発見したリスク源となり得る脅威や脆弱性、影響を受ける維持すべきサービスレベル、脅威や脆弱性から生じ得る事象に鑑みてリスクを特定(リスク特定)する。

特定したリスクについて、定性又は定量的な分析(リスク分析)を行い、事業にどのような損害を与えるかといった具体的な影響を決定する。

リスク特定及びリスク分析の結果については、前述の「Plan(準備)」のリスク評価及びリスク対応にて用いる。

4.3.1.1 内部監査や外部監査を通じた課題抽出

(1) 情報セキュリティ対策の自己点検

情報セキュリティ責任者は、年度自己点検計画に基づき、取扱者に自己点検の実施を指示すること。

取扱者は、情報セキュリティ責任者から指示された自己点検票及び自己点検の手順を用いて自己点検を実施すること。

情報セキュリティ責任者は、自己点検結果の分析を行い、情報セキュリティ関係規程や情報セキュリティ対策の更新に活用すること。

（2） 情報セキュリティ対策の監査

情報セキュリティ監査を実施する者は、監査実施計画に従って監査を実施し、事業者内基準が本ガイドラインに準拠しているか否か、及び被監査部門における実際の運用が情報セキュリティ関係規程に準拠しているか否かを確認すること。

また、監査結果は、報告書として文書化した上で、適切な保管・管理を実施すると共に、報告結果を情報セキュリティ関係規程や情報セキュリティ対策の更新に活用すること。

4.3.1.2 IT に係る環境変化に伴う脅威のための対策

平時からの情報収集に努めるとともに、新たな脅威が顕在化した時点で速やかに検討体制が構築できる準備を行うこと。

4.3.2 「障害発生時」の観点

既存の情報セキュリティ対策の運用を通じて、発見したリスク源となった脅威や脆弱性、影響を受けた維持すべきサービスレベル、脅威や脆弱性から生じた事象及びその結果を分析し、リスクとして特定すること。

5. 参考文献

本「安全ガイドライン」では、「重要インフラにおける情報セキュリティ対策の優先順位付けに係る手引書（第1版）」（以下「手引書」という。）を別冊としている。

重要インフラ事業者が、本ガイドライン 4.3「「Check（確認）・Act（是正）」の観点」を実施するにあたり、手引書の解説や取組例を参考にすることで、自らの防護対策の有効性を高めていくことを期待する。

6. 用語集

本「安全ガイドライン」において定義されている用語を以下に掲載する。

6.1 IT障害

ITの不具合のうち、重要インフラサービスの提供水準が第3次行動計画の「別紙2　重要インフラサービスとサービス維持レベル」における「サービス維持レベル」を下回るもの。

6.2 利用者

(1) 重要インフラ利用者

鉄道事業者が提供する重要インフラのサービスを利用する者を指す。

(2) 取扱者

鉄道事業者が保有する重要インフラに関する情報システム及び情報資産を取り扱う鉄道事業関係者を指す。

6.3 情報システム及び情報資産

(1) 情報システム

情報システムとは、ハードウェア及びソフトウェアから成るシステムであって、情報処理及び通信の用に供するものをいう。サーバ装置、端末、通信回線装置、複合機、特定用途機器、ソフトウェアが含まれる。

(2) 情報資産

情報資産とは、以下の情報を指す。

- 取扱者が業務上使用することを目的 として事業者が調達し、又は開発した情報システム若しくは 外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）
- 事業者が調達し、又は開発した情報システムの設計又は運用管理に関する情報

6.4 サービス不能攻撃対策

(1) パケットフィルタリング

ファイアウォールの一種で、ポート番号や発着信アドレスによってパケットの通過可否を判断する方式。もう１つの方式であるアプリケーション・ゲートウェイ方式に比べて簡易で、負荷が小さい。

出典：警察庁「＠police」用語集
（https://www.npa.go.jp/cyberpolice/words/）

（2） 3-way handshake

TCP 接続の開始手順。送信側から通信の開始要求（SYN パケット）を受信側に送ると、受信側は応答（SYN/ACK パケット）を返信する。それに対して送信側が応答（ACK パケット）を返すことにより、TCP 接続が確立される。3つのパケットが行き来することから「スリーウェイ」と呼ばれる。

出典：警察庁「＠police」用語集
（https://www.npa.go.jp/cyberpolice/words/）

（3） Flood 攻撃

大量のパケットを送信することにより攻撃先のネットワークデバイスやサーバに負荷をかける攻撃である。悪用するパケットの種類によって、「SYN Flood」「UDP Flood」「Ping Flood」「Connection Flood」等の種類がある。

出典：警察庁「DoS/DDoS 対策について」（平成 15 年 6 月 3 日）
（https://www.npa.go.jp/cyberpolice/server/rd_env/pdf/DDoS_Inspection.pdf）

（4） アプリケーションゲートウェイ

ファイアウォールの一種で、アプリケーション（サービス）の内容まで立ち入って検査する方式。もう1つの方式であるパケット・フィルタリング方式に比べて、より詳細な検査が可能である反面、負荷がかかるため大きな処理能力が必要とされる。

出典：警察庁「＠police」用語集
（https://www.npa.go.jp/cyberpolice/words/）

6.5 多要素認証機能

多要素認証とは、以下の認証方式を複数組み合わせた認証方式のことである。

- 対象者の知識を利用したもの（ID/パスワード、暗証番号、事前に登録した質問事項への回答など）
- 対象者の持ち物を利用したもの（セキュリティトークン、ICカードなど）
- 対象者の身体の特徴を利用したもの（指紋認証、静脈認証など）

6.6 ウェブアプリケーションの脆弱性

本章は、一般的なセキュリティ用語の解説であるため、解説中の「利用者」については特定の重要インフラに限らない、一般的な情報システムの利用者を指す。

（1） SQL インジェクション脆弱性

ウェブアプリケーションのプログラムがデータベースを操作する手段として SQL 言語を用いている場合に、プログラムが SQL 文を文字列の連結によって動的に生成する構造になっていると、外部か

ら悪意ある者によって与えられた攻撃用の文字列が SQL 文に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、データベースを破壊されたり、データベース内の情報を盗まれたりするなどの被害が生じ得る。このような欠陥は一般に「SQL インジェクション脆弱性」と呼ばれている。SQL インジェクション脆弱性を排除するには、SQL 文の組み立てにプレースホルダを用いる実装方法を採用することを徹底するなどの対策が考えられる。

(2) OS コマンドインジェクション脆弱性

ウェブアプリケーションのプログラムが OS のコマンドを操作する必要がある場合に、プログラムが OS のシェルのコマンドラインを用いてコマンド呼出しをする構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列がコマンドラインに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、サーバに侵入される被害が生じ得る。このような欠陥は一般に「OS コマンドインジェクション脆弱性」と呼ばれている。OS コマンドインジェクション脆弱性を排除するには、OS コマンドの操作にシェルのコマンドラインを用いない実装方法を採用することを徹底するなどの対策が考えられる。

(3) ディレクトリトラバーサル脆弱性

ウェブアプリケーションが使用するファイルのパス名を外部のパラメータから指定する仕様になっている場合に、指定されたパス名をプログラムがそのまま使用する構造になっていると、公開を想定しないファイルが参照されて、その内容が外部から閲覧され得る欠陥となる場合がある。このような欠陥は一般に「ディレクトリトラバーサル脆弱性」と呼ばれている。ディレクトリトラバーサル脆弱性を排除するには、外部のパラメータからパス名を指定する仕様を排除する対策、それができない場合には、ファイルにアクセスする直前に、使用するパス名の妥当性検査を行う方法、又は、ファイルのディレクトリと識別子を固定にしてアクセスするなどの対策が考えられる。

(4) セッション管理の脆弱性

ウェブアプリケーションのプログラムがログイン機能を有するなど、セッション管理の仕組みを持つ場合に、そのセッション管理の実装方法に欠陥がある場合がある。例えば、セッション管理に用いられるセッション ID が推測可能な値となっている場合、セッション ID を URL パラメータに格納している場合、SSL(TLS)を使用しているセッションの管理に用いる cookie に secure 属性がセットされていない場合等が、この脆弱性に該当する。この欠陥を攻撃されると、正規の利用者がログイン中に、その利用者になりすまして不正にアクセスする「セッションハイジャック」の被害が生じ得る。この脆弱性を排除するには、暗号論的疑似乱数生成器(CSPRNG)で生成する十分な長さの文字列をセッション ID として推測困難なものとし、secure 属性のセットされた cookie にこれを格納することでセッション ID の漏えいを防ぐ対策方法が考えられる。

(5) アクセス制御欠如と認可処理欠如の脆弱性

ウェブアプリケーションがログイン機能を有し、ログイン中の利用者にのみ利用を許可すべき機能がある場合に、ログインしていない利用者にもその機能が利用できてしまう欠陥がある場合がある。この

ような欠陥は一般に「アクセス制御欠如の脆弱性」と呼ばれる。また、ログイン中の利用者のうち、一部の利用者にのみ利用を許可すべき機能がある場合に、それ以外の利用者にもその機能が利用できてしまう欠陥がある場合がある。このような欠陥は一般に「認可処理欠如の脆弱性」と呼ばれる。これらの欠陥を攻撃されると、秘密情報の漏えい、なりしまし操作等の被害が生じ得る。これらの脆弱性を排除するには、アクセス制御と認可処理が必要な画面の仕様を明確にし、仕様に沿った実装を徹底するなどの対策が考えられる。

(6) クロスサイトスクリプティング脆弱性

ウェブアプリケーションのプログラムがHTMLページを出力する場合に、プログラムがHTMLを文字列の連結によって動的に生成する構造になっていると、外部から悪意ある者によって与えられた攻撃用の文字列が HTML に不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、cookieの値を盗まれてセッションハイジャックされるほか、画面の内容を改ざんされるなどの被害が生じ得る。このような欠陥は一般に「クロスサイトスクリプティング脆弱性」と呼ばれている。クロスサイトスクリプティング脆弱性を排除するには、以下を含む対策が考えられる

- HTMLの出力に際してHTMLタグの出力以外の全ての出力において文字列をHTMLエスケープ処理することを徹底する。
- URLを出力するときは「http://」又は「https://」で始まるURLのみを許可する。
- SCRIPT 要素の内容を動的に生成しないようにする。
- スタイルシートを任意のサイトから取り込める仕様を排除する。
- 全てのページについてHTTPレスポンスヘッダの「Content-Type」フィールドの「charset」に文字コードの指定を行う。

ただし、当該ウェブアプリケーションの仕様の都合で、これらだけでは解決できない場合もあり、その場合には追加的な対策が必要となる。

(7) クロスサイトリクエストフォージェリ脆弱性

ウェブアプリケーションが、ログイン中の利用者にのみ利用を許可する機能を有している場合に、その機能のウェブページに「アクセス制御欠如と認可処理欠如の脆弱性」の対策が施されている場合であっても、外部のサイトから当該ウェブページにリンクを張る方法により、利用者本人にそのリンクをたどらせることで、当該利用者の意図に反して当該機能が利用されてしまうという構造になっている場合がある。このような欠陥は一般に「クロスサイトリクエストフォージェリ脆弱性」と呼ばれている。この欠陥を攻撃されると、悪意ある者が仕掛けたリンクによって、不正に当該機能を操作される被害(具体的には、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害)が生じ得る。この脆弱性を排除するには、外部からのリンクによって機能が作動してはならないウェブページは、処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行するように実装するなどの対策方法が考えられる。

(8) クリックジャッキング脆弱性

ウェブアプリケーションが、サイト内のボタンやリンクをクリックするだけで作動する機能を有している場合に、悪意ある者が、当該サイトを透明化した（透明色で表示して利用者の目に見えないように設定された）フレームとして外部のサイト上に表示するようにし、利用者を当該外部サイトへ誘導して、当該ボタンやリンクの表示された画面上の位置をクリックさせるよう誘導することで、利用者の意図に反して当該機能を作動させることができてしまう場合がある。このような欠陥は一般に「クリックジャッキング脆弱性」と呼ばれている。この欠陥を攻撃されると、ウェブアプリケーションに設定された個人設定の内容を変更されるなどの被害が生じ得る。この脆弱性を排除するには、ウェブサーバの設定で、HTTP レスポンスに「X-Frame-Options」ヘッダを出力するようにし、そのフィールド値に「deny」又は「sameorigin」の値をセットすることで、当該ウェブページが外部のサイトにフレームとして表示されることを拒否するよう利用者のブラウザに指示する機能を用いるといった対策方法が考えられる。

（9）メールヘッダインジェクション脆弱性

ウェブアプリケーションが電子メールを送信する機能を有し、その宛先となる電子メールアドレスをウェブアプリケーションのパラメータから指定する構造になっている場合に、悪意ある者により任意の電子メールアドレスが当該パラメータに与えられ、迷惑メールの送信のために当該ウェブアプリケーションが悪用されてしまうという被害が生じ得る。この欠陥を排除するには、電子メールの送信先電子メールアドレスはプログラム中に固定的に記述する実装方法（又は設定ファイルから読み込む実装方法）を採用して、ウェブアプリケーションのパラメータを用いるのを避けるなどの対策方法が考えられる。

（10） HTTP ヘッダインジェクション脆弱性

ウェブアプリケーションが HTTP レスポンスヘッダの「Location」や「Set-Cookie」のフィールド値を動的に出力する構造になっている場合、外部から悪意ある者によって与えられた改行文字を含む攻撃用の文字列が HTTP レスポンスヘッダに不正に混入し得る欠陥となることがある。この欠陥を攻撃されると、クロスサイトスクリプティング脆弱性の場合と同じ被害が生じ得る。このような欠陥は一般に「HTTP ヘッダインジェクション脆弱性」と呼ばれている。HTTP ヘッダインジェクション脆弱性を排除するには、HTTP レスポンスヘッダを出力する際に、直接にヘッダ文字列を出力するのではなく、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用 API を使用する実装方法を採用するなどの対策が考えられる。

（11） eval インジェクション脆弱性

ウェブアプリケーションのプログラムを作成する言語が、「eval」等、文字列をプログラムとして実行する機能を持つ言語である場合に、プログラムがこの機能を使用していると、外部から悪意ある者によって与えられた攻撃用の文字列が、その eval に与える文字列に混入し得る欠陥となることがある。この欠陥を攻撃されると、任意のプログラムがサーバで実行されることとなり、様々な被害が生じ得る。このような欠陥は一般に「eval インジェクション脆弱性」と呼ばれる。この脆弱性を排除するには、eval 機能を一切使用しない実装方法を採用するなどの対策が考えられる。

（12）　レースコンディション脆弱性

ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、一方の利用者向けの処理ともう一方の利用者向けの処理を途中で取り違えてしまう事態が一定の確率で発生する場合がある。このような欠陥は一般に「レースコンディション脆弱性」と呼ばれる。この欠陥により、利用者の秘密にすべき情報が第三者に閲覧される被害が生じる。この被害は、攻撃者がいなくても偶然に発生する場合もあれば、攻撃者が大量のアクセスをすることで意図的に引き起こされる場合もある。この脆弱性を排除するには、ソースコードレビューによってレースコンディションが起きえない構造にプログラムが記述されていることを確認する方法や、大量のアクセスを同時に発生させて異常が発生しないことを十分に確認するテストを行うなどの対策方法が考えられる。

（13）　バッファオーバーフロー及び整数オーバーフロー脆弱性

ウェブアプリケーションのプログラムを作成する言語として、バッファオーバーフロー脆弱性等が生じない言語を採用することが望ましいが、その場合であっても、ウェブアプリケーションが、内部で C 言語等を用いて独自に作成されたプログラムを呼び出す構造になっている場合がある。その呼び出されるプログラムにバッファオーバーフロー脆弱性や整数オーバーフロー脆弱性が存在し、ウェブアプリケーションに外部から与えた文字列が当該プログラムに引き渡される構造になっていると、それらの欠陥を攻撃されて、サーバに侵入される被害が生じ得る。このような脆弱性を排除するためには、C 言語等のバッファオーバーフロー脆弱性等が生じ得る言語により作成されたプログラムが内部で呼び出されることを避けるなどの対策が考えられる。

【改訂履歴】

平成18年　9月29日　　制　定
平成24年10月29日　　一部改訂（第2版）
平成28年　4月　1日　　一部改訂（第3版）