情報セキュリティポリシーの策定について

近年のインターネットの爆発的な普及により、わたしたちの生活でもコンピュータを利用する機会が増えてきております。インターネットは大変便利である反面、コンピュータウィルス等の被害も増加しています。また、ネットワークを利用した犯罪や情報漏洩等も大きな問題となっています。

こうした背景の中で、朝日町は、行政で扱う個人（住民）情報や行政における重要決定事項等の情報資産の重要性を考え、行政を継続的に安定したものにするための適切なセキュリティ対策の実施が不可欠と考え、情報資産の機密性、完全性、可用性を確保するために、全庁的な統一指針として「情報セキュリティポリシー」を策定しました。

■朝日町情報セキュリティポリシー基本方針（ＰＤＦファイル）

情報セキュリティポリシーの概要

① ポリシーとは？

どのような情報資産をどのような脅威から、どのようにして守るかについての基本的な考え方、情報セキュリティを確保するための体制、組織及び運用を含めた規定であります。

② ポリシーの構造は？

◇ **基本方針**

情報セキュリティ対策に対する根本的な考え方を表し、情報資産をどのような脅威から守るかを明確に述べたものです。

◇ **対策基準**

基本方針に定められた情報セキュリティを確保するために、遵守すべき行為及び、判断の基準を示したものです。

◇ **実施手順**

対策基準に定められた内容を具体的に適用するための実施方法・手順を明文化したものです。

情報セキュリティ基本方針

朝　日　町

序文

高度情報化社会と言われ、行政事務における IT（情報通信技術）の活用により、利便性は大きく向上してきています。その反面、情報の不正アクセスやコンピュータウイルス等の発生により、情報セキュリティが脅かされる可能性も増えてきています。

こうした背景の中で、朝日町は、行政で扱う個人（住民）情報や行政における重要決定事項等の情報資産の重要性を考え、行政を継続的に安定したものにするための適切なセキュリティ対策の実施が不可欠と考えます。

情報資産の機密性、完全性、可用性を確保するために、全庁的な統一指針として「情報セキュリティポリシー」を策定し、実施します。

具体的には、

- 住民及び顧客から預託された情報並びに当町が保有する情報は、適切な保護対策を講じ、漏洩、改ざん、破壊等から守ります。
- 情報資産を取扱う関係者全員に対して、情報セキュリティの重要性の認識、情報資産の適正な利用を周知徹底し、法令遵守意識の向上に努めます。
- 情報セキュリティポリシーの遵守状況を監視及び評価するために、セキュリティ監査を実施し、継続的改善に努めます。

平成１７年４月１日

朝日町長　田代　兼二朗

第１章　本書の目的

第１節　本書の目的

本書は、情報セキュリティポリシーの構成文書の一つである基本方針として、当町の職員及び業務委託事業者等の情報資産を扱う者全員が、情報資産を使用するときに従うべき、情報セキュリティを守るための基本的な考え方や方向性を定めるものである。

第２節　適用範囲

本書は当町が管理する全業務に適用する。
対象とする組織は、町長部局、議会、教育委員会とする。
対象とするシステムの範囲は、当町が管理するすべてのコンピュータシステム、ネットワークシステム、並びにそれらで取扱う電磁データ及び入出力電磁媒体とする。

第３節　用語定義

(1) 機密性
アクセスを許可された者だけが情報にアクセスできることを確実にすること。

(2) 完全性
情報及び情報処理が、正確であること及び完全であることを保護すること。

(3) 可用性
認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

(4) 情報セキュリティ
情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持すること。

(5) ネットワーク
当町におけるシステムを相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組み。

(6) 情報システム
ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成された情報を処理する仕組み。

(7) 情報資産
情報システム及びその開発・運用等に係る各種文書類、職務において作成又は取得した文書、図画及び磁気テープや磁気ディスクその他これに類する媒体に記録された情報。

(8) 職員

当町の正職員及び臨時職員。

(9) 情報セキュリティ管理者
主管する業務において、情報を収集、作成、又は住民等の第三者から情報を預託された部門の所属長をいう。当町では各課等長がこの任にあたる。

(10) 重要情報資産
セキュリティ面で何らかの管理が必要な情報資産。使用許可を得た入出力媒体等もこれに含む。

第２章　基本的な考え方

第１節　情報資産に関する脅威

情報資産に対する脅威の発生度合や発生した場合の影響の大きさを考慮すると、特に認識すべき脅威は以下のとおりである。

(1) 外部からの不正アクセス又は不正操作によるデータ又はプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難等

(2) 職員及び業務委託事業者による誤操作、不正アクセス又は不正操作によるデータ又はプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等

(3) 地震、落雷、火災、風水害等の災害によるサービスの停止

(4) 事故、故障、障害等によるサービスの停止

第２節　セキュリティレベル

前節で示した脅威から情報資産を保護するために、情報が不当に他者に漏洩しない（機密性）、情報が改ざんされない（完全性）、障害発生時にも継続して提供できる（可用性）の３つの側面を定義する。
情報資産の重要度に応じて、情報資産の機密性、完全性及び可用性を維持するために、セキュリティレベルを設定する。
セキュリティレベルごとに情報資産の保護管理要件を明確にし、想定されるリスク及びその対策を明確にする。

第３節　情報セキュリティ対策

３つの側面から情報資産の重要性を検討し、以下の情報セキュリティ対策を講ずることとする。

(1) 人的対策
情報セキュリティに関する権限及び責任を定め、職員等に基本方針及び情報セキュリティに関する法令等の内容を周知徹底する等、十分な教育及び啓発が行われるよう必要な対策を講ずる。

(2) 物理的対策

情報システム及びネットワークを設置する施設への不正な立ち入り、並びに情報システム、ネットワーク及び情報資産への損傷・妨害等から保護するための物理的な対策を講ずる。

(3) 技術的対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を講ずる。

(4) 開発・運用上の対策

情報システム開発の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等、開発・運用面の対策を講ずる。

また、緊急事態が発生した場合に速やかな対応を可能とするための危機管理対策を講ずる。

第３章　情報セキュリティポリシー等の取り扱い

情報セキュリティポリシーは、当町が管理する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置する。

従って、町長をはじめとして当町が管理する情報資産に関する業務に携わる全ての職員及び業務委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

第１節　基本方針

基本方針は、住民の個人情報及び行政運営上の情報の管理及び情報セキュリティ対策についての基本的な考え方や方向性を定める。外部に対し公開する。

第２節　対策基準

基本方針に基づいた情報セキュリティ対策を講じるに当たって、遵守すべき行為、判断等の基準を統一的に定めるために、必要となる基本要件を明記した対策基準を定める。

対策基準は、当町の情報資産を扱うすべての職員及び業務委託事業者に対し、周知徹底する。対策基準は、公にすることにより当町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

第３節　実施手順

情報セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の部署や情報システムについて具体的な手順を明記した実施手順を定める。

実施手順は、公にすることにより当町の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

第４節　情報セキュリティポリシーの改訂

情報セキュリティを取り巻く状況の変化に速やかに対応するため、情報セキュリティ監査の結果等も踏まえ、情報セキュリティポリシーは定期的に見直し、必要に応じて改訂する。

第４章　情報資産

第１節　情報資産の分類

情報セキュリティ管理者は、情報資産を重要度に応じてセキュリティレベルに分類しなければならない。

第２節　保護管理要件の決定

情報セキュリティ管理者は、情報資産のセキュリティレベルを明示し、必要な場合は、追加の保護管理要件を設定し、想定されるリスク及びその対策を明確にしなければならない。

第３節　情報資産の取扱い

情報資産の利用者は、情報資産に定められたセキュリティレベルに従って取り扱わなければならない。さらに、情報セキュリティ管理者が追加して定めた保護管理要件に従わなければならない。

第５章　人的対策

第１節　職掌上の役割と責任

第１項　　町長の役割と責任

町長は、情報セキュリティに関する指針を明らかにし、職員及び業務委託事業者に対して情報セキュリティ意識を浸透させ、必要な支援を行わなければならない。

第２項　　課等長の役割と責任

課等長は、情報セキュリティ確保の責任を負い、部下及び業務関係者が情報セキュリティポリシーを理解し遵守することを徹底し、かつ管理しなければならない。

また、課等長は、所属部署の職員が退職、異動又は業務変更する場合、及び業務委託事業者が契約終了した場合、利用する必要のなくなった全ての情報資産を回収しなければならない。

第３項　　職員の役割と責任

職員は、情報セキュリティポリシー及び課等長の指示を遵守し、情報が不正な手段で取得されること又は不正に使用されることを防止しなければならない。
職員は、退職、異動又は業務変更する場合に利用する必要のなくなった全ての情報資産を当町に返却しなければならない。

第４項　業務委託事業者の役割と責任

業務委託事業者は、契約に基づき情報セキュリティポリシー及び関係する部署の課等長の指示を遵守し、情報を不正な手段で取得したり、不正に使用してはならない。
業務委託事業者は、契約終了その他を原因として当町の情報資産を取扱うことがなくなった時点で、全ての情報資産を当町に返却しなければならない。

第２節　情報セキュリティ上の役割と責任

情報セキュリティ確保のため、情報セキュリティ管理者、情報システム管理者、利用者の３つの役割と責任を定める。

情報セキュリティ管理者は、自らが所有する情報資産を把握し、その重要度の判断を行い、セキュリティレベルを決定し、いかに管理するかを決定した上で情報システム管理者に通知しなければならない。
情報システム管理者は、所属部署の職員及び業務委託事業者が当町情報セキュリティポリシーを理解し、遵守していることを管理しなければならない。また、情報セキュリティ管理者の指示に基づき所属部署での情報資産の保護・管理を行わなければならない。
利用者は、情報セキュリティ管理者及び情報システム管理者の指示に基づいて情報資産を使用しなければならない。

第３節　情報セキュリティ管理組織

情報セキュリティ管理組織は情報セキュリティ統括責任者と情報セキュリティ委員会で構成する。

第１項　情報セキュリティ統括責任者

当町における情報セキュリティ対策の責任者である町長がこの責務にあたる。情報セキュリティ統括責任者は情報セキュリティ管理組織のトップに位置し、情報セキュリティ委員会のメンバーを任命する。

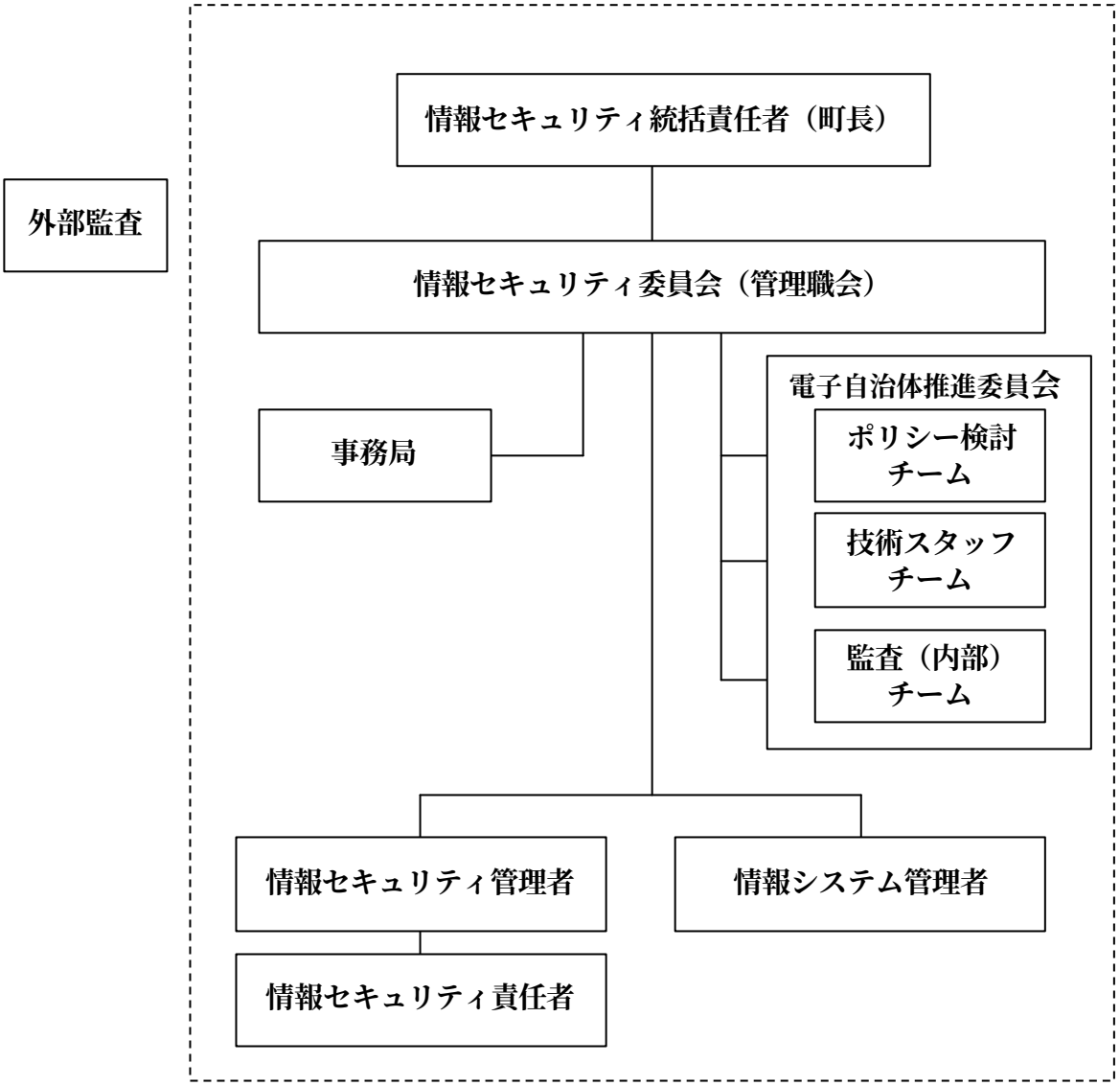
第２項　情報セキュリティ委員会（管理職会）

(1) 情報セキュリティポリシーを管理し、変更が必要と判断された場合は、基本方針、対策基準、実施手順の見直しを行う。
(2) 当町の情報セキュリティに関する情報を収集し、情報セキュリティ対策の討議を行い、情報セキュリティ統括責任者を補佐する。
(3) 想定されるリスクの判定やリスクの査定等、方針から外れる特殊な要件についての判断を行う。
(4) 情報セキュリティポリシーを円滑に管理・運用していくために技術的な

側面で支援を行う。

(5) 情報セキュリティポリシーが遵守されていることを監査する。

情報セキュリティ管理組織図



第４節　情報セキュリティに関する教育

情報セキュリティポリシーの職員及び業務委託事業者への浸透と情報セキュリティ意識向上のため、情報セキュリティに関する教育を実施する。

第５節　第三者による情報資産使用に関する方針

業務委託事業者等第三者が当町の重要情報資産を使用する場合は、情報セキュリティ管理者が事前に情報セキュリティ統括責任者に情報資産使用を報告しなければならない。また、使用前に情報セキュリティ上必要な事項について、その第三者と契約を締結する。

第６章　物理的対策

第１節　セキュリティエリア

不正侵入や業務への割り込みを防御するために、重要情報資産をもつ情報システムが存在するフロアには物理的な保護エリアを設定し、管理責任者を定めた上で管理を行わなければならない。

第２節　情報機器管理

情報機器の設置、廃棄及び移動については、適切な管理を行わなければならない。

第７章　技術的対策

第１節　識別と認証

利用者は識別子（ID、カード等）と固有の認証子（パスワード等）を使用しなければならない。識別子と認証子は他の利用者と共有してはならない。また、識別・認証を確実に行えるように設定間隔、誤入力の取扱いを定め、管理された状態に置かなければならない。

第２節　アクセス制御

利用者は情報資産のセキュリティレベルに従い、承認された者のみが情報システムに対してアクセスが可能であるように制御しなければならない。

第３節　不正ソフトウェアからの保護

悪意のあるソフトウェアから保護するための検出及び防止の管理を行わなければならない。

第８章　開発・運用上の対策

第１節　情報システム運用管理

情報システムの運用手順、事故管理手順を文書化し、その手順に基づいて適切に管理運用しなければならない。

第２節　情報システム開発及び保守

第１項　　情報システム開発

情報システムを開発する前には情報セキュリティ要件を明確にし、その要件に基づいて開発を行わなければならない。

第２項　　情報システム開発・保守環境

情報システムの開発環境及び保守環境は、運用システムの環境と分離しなければならない。

第９章　緊急時対応計画の策定

主要業務毎にセキュリティレベルに基づいた、非常時の手順、バックアップ手順、業務再開手順等を含む緊急時対応計画を策定しなければならない。
緊急時対応計画は定期的にテストを行い、計画の有効性を確認し、適宜見直さなければならない。

第１０章　　ポリシーの遵守

第１節　法令遵守

職務を遂行するに当たり、使用する情報資産について、関連する法令等を遵守し、これに従わなければならない。

第２節　点検

情報セキュリティポリシーに沿った情報セキュリティ対策が実施されているかどうか、定期的に点検を行わなければならない。

第３節　情報セキュリティ監査

情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査を行わなければならない。

第４節　罰則

職員が、情報セキュリティポリシーに違反した場合は、その重大性、発生した事案の状況に応じて地方公務員法等の定めにより懲戒処分等の対象とする。
業務委託事業者が、情報セキュリティポリシーに違反した場合の対応については、予め業務委託契約に定めておかなければならない。