総社市情報セキュリティ基本方針

1　目的

近年の情報通信技術の飛躍的な発展は，社会や経済，住民の生活に対して大きな影響を与えており，行政においても高度ＩＴ化への取り組みが進められている。このような情報環境の変化への対応として，総社市では市内の公共施設を光ファイバー網で結ぶとともに，これを岡山情報ハイウェイに接続するなどして，住民がインターネットを快適に利用できる環境をいち早く整備し，住民との情報の共有による行政業務の効率化にも積極的に取り組んでいる。

一方で，ネットワークに接続された情報システムは，不正アクセスによる盗聴・破壊・改ざん等の脅威に常にさらされている。また，住民の個人情報や行政業務で扱う機密情報についても漏えい・改ざん等の脅威が潜在している。こうしたさまざまな情報セキュリティ上の脅威に対しては技術的な対策はもとより，人的なセキュリティ対策も重要であり，住民のプライバシーや財産を守るために必要なシステムの構築が求められている。

そこで，総社市の情報資産が個人の裁量によって扱われることのないよう，情報セキュリティに対する総社市の基本的な取り組みを明確にした『情報セキュリティポリシー』を策定する。そして，このポリシーを推進する枠組みとしての『情報セキュリティマネジメントシステム』を確立し，総社市における情報セキュリティを継続的に維持するとともに，不断の見直しによる情報セキュリティの向上を目指すものとする。

総社市のすべての職員が『情報セキュリティポリシー』を遵守することで，行政業務の効率化のみならず，住民が安心して利用できる行政サービスの質の向上に努めるため，この基本方針となる「情報セキュリティ基本方針」をここに定める。

2　定義

(1) 情報資産

情報や情報システム，及びこれらを保護，使用するために必要なものをいう。データ（媒体を問わない），ハードウェア，ソフトウェア，ネットワーク，建物・設備等が含まれる。

(2) 情報セキュリティ

情報資産の機密性・完全性・可用性（注）を維持することをいう。

（注）：国際標準化機構（ISO）が定めるもの（ISO 7498－2：1989）

機密性（confidentiality）　：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）　：情報および処理の方法の正確さと，完全である状態を完全防護すること。

可用性（availability）　：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

(3) 情報セキュリティマネジメントシステム

管理体制の整備，守るべき情報セキュリティレベルの明確化，情報セキュリティ対策の実施，情報セキュリティ対策の実施状況の定期的な評価等を，組織として継続的に行っていく管理の枠組み。

3　情報セキュリティポリシーの位置づけ

情報セキュリティポリシーは，総社市の情報セキュリティマネジメントシステムの根幹をなすものであり，総社市の情報資産をセキュリティ上の脅威から保護するための情報セキュリティ対策について総合的・体系的にまとめたものである。

4　情報セキュリティポリシーの構成

情報セキュリティポリシーは，「情報セキュリティ基本方針」と「情報セキュリティ対策基準」の２階層から構成される。（下図参照）

また，情報セキュリティポリシーに基づき，具体的な情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を別に策定することとする。

・情報セキュリティ基本方針

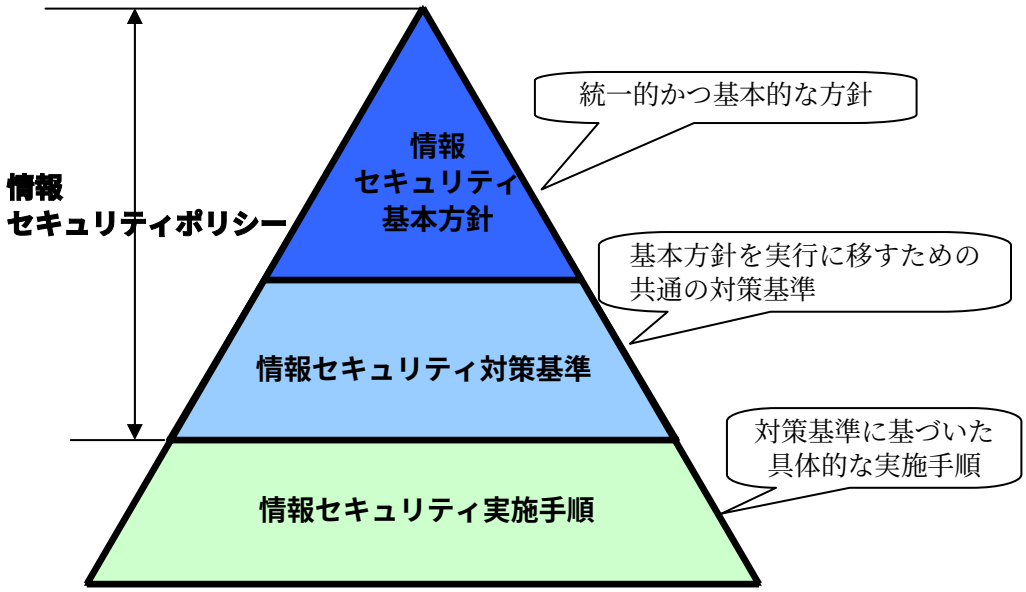
情報セキュリティ対策に関する基本的な方針を定めたもの

・情報セキュリティ対策基準

情報セキュリティ基本方針に基づく対策基準を定めたものであり，管理の種別ごとに規程としてまとめたもの

・情報セキュリティ実施手順

情報セキュリティ対策の具体的な実施手順であり，情報セキュリティ対策を実施する部門内で個々の情報資産ごとに定め，情報セキュリティポリシーに基づく情報セキュリティ対策を，業務において具体的に実施するためのもの



5　適用範囲

情報セキュリティポリシーは，総社市の保有するすべての情報資産並びに情報資産を扱うすべての職員に対して適用する。

6　職員の責務

総社市の情報資産に接するすべての職員は，情報セキュリティの重要性について共通の認識をもつとともに，情報資産の利用にあたって情報セキュリティポリシーを遵守しなければならない。

7　情報セキュリティマネジメントの体制

総社市の情報セキュリティを確保するために全庁にわたる管理体制を以下に定める。

・情報セキュリティ統括責任者

情報セキュリティマネジメントシステム全般に関する責任と権限を有し，総社市における情報セキュリティを統括する。

・情報セキュリティ責任者

情報セキュリティポリシーに基づくリスク評価，管理策の実施および見直し，教育訓練等を推進する。

・情報セキュリティ委員会

総社市の情報セキュリティを維持し，全庁的なマネジメント体制を整えるとともに，情報セキュリティポリシーの承認などセキュリティに関する重要な事項を審議する。

8　情報資産の分類と管理

総社市の情報資産に対し，機密性・完全性・可用性の観点から重要度を検討するとともに，脅威の発生頻度および発生した脅威が被害に結びつく可能性から求めたリスクに応じて情報資産の分類を行い，必要かつ十分な情報セキュリティ対策を行うものとする。

9　情報セキュリティ対策

総社市の情報資産をセキュリティ上の脅威から保護するために，以下に示す情報セキュリティ対策を実施する。具体的な対策は，情報セキュリティ対策基準に明示される。

(1) 人的セキュリティ対策

情報セキュリティに関する権限と責任を明確に定めるとともに，情報セキュリティポリシーを全職員が理解・実践できるように教育と訓練を計画的に実施する。

(2) 物理的セキュリティ対策

施設や室への不正侵入や，配線を通じた盗聴，盗難・破壊・損傷等の脅威から情報資産を保護するため，入退室管理や機器管理等の物理的対策を実施する。

(3) 技術的セキュリティ対策

外部からの不正アクセスやウィルスによる被害から情報資産を保護するために，アクセス制御，ネットワーク管理，ウィルス対策等の技術的な対策を実施する。

(4) 運用におけるセキュリティ対策

情報漏えいや，障害・緊急事態による業務中断の長期化等を防止するため，ネットワーク監視，業務委託管理，情報セキュリティポリシーの遵守状況の確認，事業継続計画の策定等，情報資産の運用面に係る対策を実施する。

１０　個人情報保護

総社市の行政業務で扱う情報資産のうち，個人情報を含むものについては，『総社市個人情報保護条例』により保護しなければならない。

１１　法令遵守

総社市の情報資産に接するすべての職員は，情報セキュリティポリシーに加え，関連する法令，条例，規則等についても遵守しなければならない。

１２　罰則

情報セキュリティポリシーに違反した職員に対しては，法令や条例に対する違反の有無，故意であったか過失・怠慢であったかの違い，情報資産に与えた被害の規模（被害金額やサービス停止期間等）に応じて罰則を適用する。

１３　評価・見直し

情報セキュリティ対策は，構築した時点では十分であっても，情報資産を取り巻く環境の変化等により不十分なものになってしまう。このため，定期的な監査を実施することで，情報セキュリティポリシーの実効性を評価し，情報セキュリティポリシーの見直しを実施する。

以上，総社市では，全職員による情報セキュリティポリシーの遵守を通じて，**「安全でにぎわいのあるまちづくり」**に取り組むものとする。

平成１６年４月

総社市長　竹内洋二

（履歴）

年　月　日	場　所	内　容
平成１６年　４月３０日　策定	－	新規策定