

今年度のガイドラインの改定方針について



総務省

令和 8 年 9 月 9 日
自治行政局 住民制度課
サイバーセキュリティ対策室

重要インフラのサイバーセキュリティ対策のための統一基準の ガイドラインへの反映について

論点②

- ガイドラインのベースであるISO/IEC27001の考え方は踏襲しつつ、「組織統治」、「識別」、「防御」、「検知」、「対応及び復旧」の各プロセスの重要性を追加する形でガイドラインの改定を検討するのはどうか。

総務省ガイドライン（現行）

ISO/IEC27001ベース

対策基準番号	項目
対策基準 1.	組織体制
対策基準 2.	情報資産の分類と管理
対策基準 3.	情報システム全体の強靱性の向上
対策基準 4.	物理的セキュリティ
対策基準 5.	人的セキュリティ
対策基準 6.	技術的セキュリティ
対策基準 7.	運用
対策基準 8.	業務委託と外部サービス（クラウドサービス）の利用
対策基準 9.	評価・見直し

- ・ 防御中心に責任者・管理者・担当者等における権限・責任等に関して記載
- ・ CISOにおけるCSIRTの整備やCSIRTの役割（報告・連絡）に関する記載は、平成30年9月改定において追記

総務省ガイドライン（改定イメージ）

ISO/IEC27001ベース+NIST CSF2.0※

+

「組織統治」、「識別」、「防御」、「検知」、「対応及び復旧」
各プロセスの重要性を追加

＜方向性＞

- ・ 基本方針に各プロセスを整備することの重要性を示しつつ、対策基準の項目は変更せず、境界防御に依拠した対策を中心に記載している「対策基準 3『情報システム全体の強靱性の向上』」の箇所を中心に追加・修正等を検討

＜主な検討内容＞

- ・ 組織におけるガバナンスの重要性や自治体においてガバナンスをどう確立していくか等を検討
- ・ 境界防御に依拠した対策において万が一境界が突破された場合におけるリスク等を明示した上で、重要な情報資産におけるサイバー攻撃等に対する耐性とレジリエンスを高めるための考え方と責任者・管理者・担当者等における役割を検討
- ・ 特に、構成管理・脆弱性管理、常時監視によるインシデント予兆等の検知、緊急時対応計画や業務継続計画等と連動した対応等について追記を検討

「重要インフラのサイバーセキュリティ対策のための統一基準」の構成①

- 重要インフラのサイバーセキュリティ対策のための統一基準は、第1部から第3部の構成となり、主に第3部に地方公共団体に係る安全基準等の事項について示されている。
- 第1部においては、目的や適用範囲を中心に記載されているが、**地方公共団体の「行政サービス」が重要インフラ分野に指定されていることを周知**するため、ガイドラインの第1編総則において新たな章を設け、**重要インフラ分野における取組みの重要性**や重要インフラの**サイバーセキュリティを確保し、レジリエンスを高めることが不可欠**である旨を示すのはいかがか。
- また、「重要インフラのサイバーセキュリティに係る安全基準策定ガイドライン」（パブリックコメント済）に示されている「講ずべき対策事項」やその解説については、ガイドラインへの反映を検討する。

章番号	重要インフラのサイバーセキュリティ対策のための統一基準		当室のセキュリティポリシー ガイドラインへの反映
	大項目	中項目または小項目	
第 1 部総則			
1.1	統一基準の目的等	(1) 統一基準の目的 (2) 統一基準による重要インフラのサイバーセキュリティ強化 (3) 統一基準と行動計画との関係 (4) 統一基準と他法令との関係	第 1 編「総則」に新たな章を作成し、 重要インフラ分野における取組みの重要性等を記載 する。
1.2	統一基準の適用範囲	—	
1.3	統一基準に基づく施策の改善	—	
1.4	統一基準の構成等	—	
1.5	統一基準の改定	—	
第 2 部 政府機関における施策の基準			
2.1	実施計画の策定	2.1.1 施策の実施体制 2.1.2 取り組むべき施策	主に国家サイバー統括室及び重要インフラ所管省庁等の政府機関における対応に関する内容であるので、ガイドラインには反映しない。
2.2	把握・分析	—	
2.3	評価・改善	—	

「重要インフラのサイバーセキュリティ対策のための統一基準」の構成②

- 第3部は、主に所管省庁や業界団体が定めるガイドライン等で規定されるべき事項が示されている。総務省のガイドラインにおいて記載されている事項も多いため、第1編または付録において、重要インフラ分野における統一基準に示された事項と総務省のガイドラインの記載頁等の対応を示すことで、関連性を分かり易く示すのはいかがか。
- 「**検知**」や「**対応及び復旧**」に関する事項は、総務省のガイドラインにおいて記載内容が十分ではないことから、対策基準の例文に追記するのはいかがか。

章番号	重要インフラのサイバーセキュリティ対策のための統一基準		当室のセキュリティポリシー ガイドラインへの反映
	大項目	中項目または小項目	
第3部安全基準等において規定されるべき事項			
3.1	基本的な考え方	(1) 目的及び位置付け (2) 記載の観点及び構成 (3) 対象範囲 (4) 関係主体の役割	第2編対策基準3.『情報システム全体の強靱性の向上』(例文・解説)において、 <u>レジリエンス、任務保証、リスクベース等の考え方を示す。</u>
3.2	組織統治	3.2.1 組織状況の理解 3.2.2 組織方針 3.2.3 組織内外のコミュニケーション 3.2.4 経営リスクとしてのサイバーセキュリティリスクの管理 3.2.5 役割・責任・権限 3.2.6 監査・モニタリング 3.2.7 情報開示 3.2.8 継続的改善 3.2.9 サプライチェーン・リスクマネジメント	第2編対策基準1.『組織体制』(例文・解説)において、 <u>組織統治に関する事項を追加し、</u> 首長や幹部層におけるサイバーセキュリティに関する関与について具体的に明示し、組織として監査・モニタリング・組織戦略として方向性を示すことの必要性を追記する。
3.3	識別	3.3.1 資産の管理 3.3.2 脅威情報及び脆弱性情報の収集・分析 3.3.3 情報共有 3.3.4 リスクアセスメント 3.3.5 サイバーセキュリティリスク対応 3.3.6 脆弱性の管理	第2編対策基準3.『情報システム全体の強靱性の向上』(例文・解説)において、これまで対策基準においては記載がない『 <u>リスクアセスメント</u> 』や『 <u>リスク対応計画</u> 』の <u>取組み</u> 等について追記する。また、攻撃者がAIを悪用するリスクを踏まえ、 <u>組織的なパッチ適用に関する方針</u> 等に関する記載を追記する。

「重要インフラのサイバーセキュリティ対策のための統一基準」の構成③

章番号	重要インフラのサイバーセキュリティ対策のための統一基準		当室のセキュリティポリシー ガイドラインへの反映
	大項目	中項目または小項目	
第3部安全基準等において規定されるべき事項			
3.4	防御	3.4.1 アカウント管理・認証・アクセス制御 3.4.2 意識向上とトレーニング 3.4.3 データのセキュリティ対策 3.4.4 システムのセキュリティ対策 3.4.5 ログ取得 3.4.6 インフラストラクチャ（ネットワーク等）の対策 3.4.7 クラウドサービス利用時の対策	概ね既に記載がされている内容であるため、ガイドラインの記載内容の表現等を見直す程度とする。
3.5	検知	3.5.1 監視・分析体制の整備 3.5.2 継続的監視 3.5.3 事象の分析	第2編対策基準7.『運用』（例文・解説）における以下の項目について見直しを行う。 攻撃を検知した際のIoC（Indicator of Compromise）の収集や情報の共有等について全般的に追記 する。 ・現在のガイドラインでは、サイバー攻撃に関する検知の観点が不足 ・侵害時におけるインシデント対応や迅速な復旧、業務継続との関係等について記載が不足 ＜7.1情報システム監視＞ ＜7.3侵害時の対応等＞
3.6	対応及び復旧	3.6.1 事業継続計画等 3.6.2 インシデントへの対応及び復旧 3.6.3 危機管理	
3.7	技術・脅威の動向等を踏まえた対策	—	AI等の悪用による攻撃の高速化・大規模化に関する対応等 については、第2編対策基準3.『情報システム全体の強靱性の向上』（例文・解説）において、レジリエンス、任務保証、リスクベース等の考え方の中で 環境の変化への対応の重要性とともに言及する。

政府機関等の対策基準策定のためのガイドラインの改定の反映について

政府機関等の対策基準策定のためのガイドラインの改定の反映

- 「政府機関等の対策基準策定のためのガイドライン」が令和8年6月に改定されたことから総務省ガイドラインに反映すべき内容を（水色枠）検討する。以下の表は、「政府機関等の対策基準策定のためのガイドライン」の改定内容と項目数(増)を示したもの。

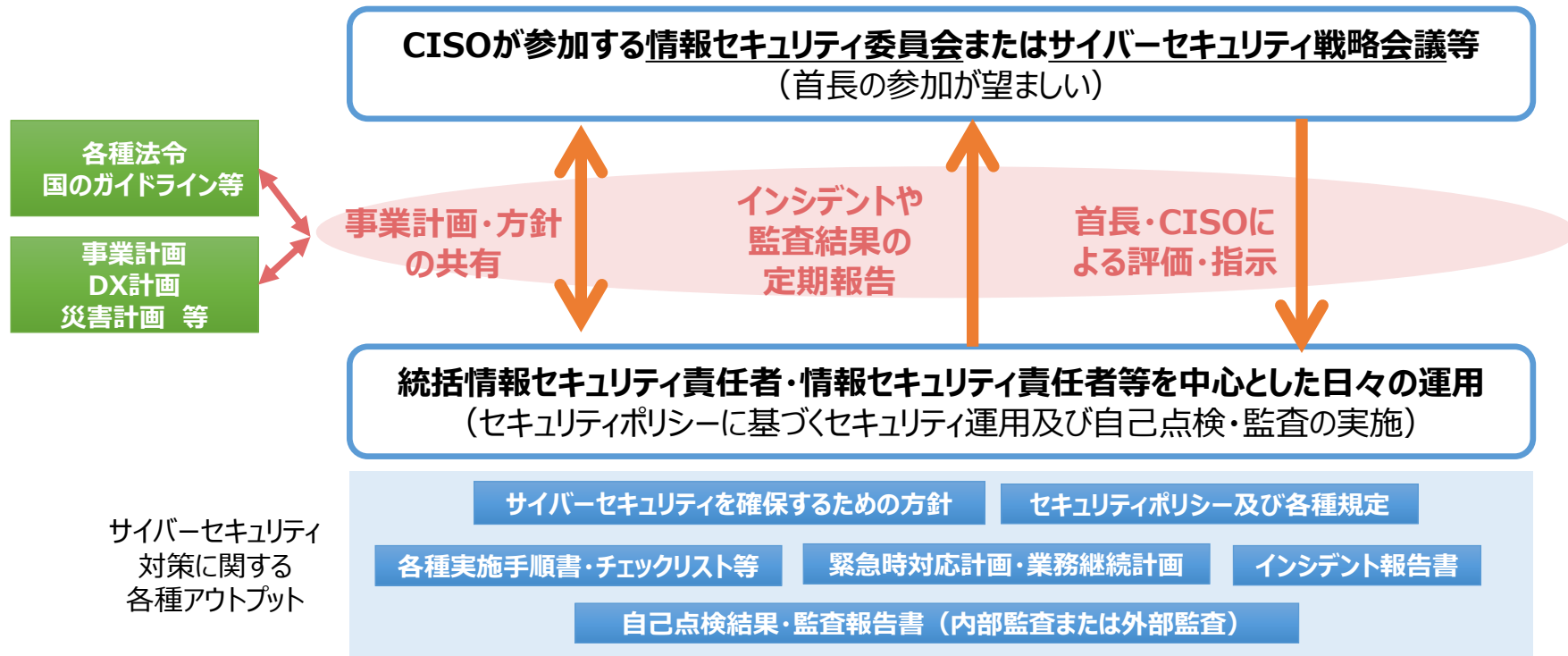
#	分類	概要	件数 (計86)	自治体 対象
1	非常時優先業務等	可用性関連の対策事項の適用対象を、「要安定情報を取り扱う情報システム」から「非常時優先業務等を支える情報システム」まで横断的に拡張。	20	×
2	主体認証	①MFA適用対象を重要システムの強権限主体まで拡大、②ウェブブラウザ経由認証でフィッシング耐性方式の導入検討を新設、③FIDO認証をMFAの方式と明確化、④PW定期変更の要求機能・関連解説を全面削除、⑤オンライン手続リスク評価を再整理、⑥本来の主体へのログイン通知機能を新設、⑦2段階認証は脆弱性を踏まえリスク受容判断を経て利用する対象と整理。	15	○
3	情報の抹消方法見直し	抹消方法の全面改訂（表3.1.1-1）。リース機器の暗号化消去のCRYPTREC準拠。暗号化消去の実施記録。クラウドサービス利用終了後の要機密情報の廃棄。 →昨年度の総務省ガイドラインにて反映済み	8	○
4	業務委託先の 情報セキュリティ対策追加	SP800-171参照範囲を拡張（Planning／Supply Chain Risk Management／System and Services Acquisitionを追加）。①委託先のインシデント対応トレーニング計画・実施、②特権アカウントのMFA必須化＋非特権への拡大、③委託先へのセキュリティポリシー・行動指針の周知、④サプライチェーンを含むリスク継続評価を新たに要求。	7	○
5	IT-BCP	統括情報セキュリティ責任者に政府業務継続計画上の非常時優先業務を支える情報システムへの該当性確認、及び運用継続計画の整備状況確認を義務化。想定する危機的事象を不正プログラム感染・サービス不能攻撃等まで拡張。作成プロセスを新規提示し、NCOガイドラインを参照先として明示。未整備時の最高責任者への整備要請・情報システム台帳による網羅管理も新設。 →サイバー攻撃に関するICT-BCPガイドラインは次年度検討予定（大規模災害に関してはR5年度済）	7	△
6	ログ取得	ログ取得の設計方針を「取得項目の列挙型」から「想定脅威の分析に基づく脅威ベース設計型」へ転換。取得目的をインシデント対応・サイバー脅威分析まで拡張し、IoC・アノマリ検知に資する情報の含有を要請。保存期間はガイドライン・リスクベースで設定するよう規定を拡充。SIEM等での一元保存時のアクセス制御要件を新設。	6	○
7	脆弱性対策の強化	パッチ適時適用を基本対策事項へ格上げし運用体制構築まで要求。脅威動向を踏まえた迅速対応判断・運用停止検討、ベンダ対応体制確認を新設。	5	○
8	情報セキュリティ インシデント対応	「IoC」の定義を新設。対処手順応急措置・復旧作業前のログ保全を明記。統括室への連絡項目に技術分析情報を追加。統括室への連絡強化の政策的根拠を明示。再発防止策の策定にフォレンジック結果・攻撃者挙動に基づく技術的検討を必須化。	5	○
9	RTO/RLO	「許容される停止時間」、「中断することのできる時間」をRTO、RLOに置換。	4	○
10	DMARCポリシー	DMARCポリシーを"p=quarantine"／"reject"設定を原則義務化。"p=none"許容の旧解説を削除し、1年以内の強化移行手順・BIMI導入推奨を新設。	3	○
11	管理者権限の付与	権限の付与と執行を同一のものが兼ねないこと。強い権限は常時付与せず承認を都度得る運用とすること。	2	○
12	JC-STAR	JC-STARのラベル★1の製品から調達を推奨すること。★3ラベルに関する通信機器、NWカメラの追加要件の確認。	1	○
13	SCS評価制度	サプライチェーン強化に向けたセキュリティ対策評価制度を活用すること。	1	○
14	情報の追記	政府機関及びその職員が申請・届出等手続において電子署名を行う際にはGPKIを使用すること。	1	×
15	人材フレームワークの活用	セキュリティ体制の具体化を検討する際には、NCO「サイバーセキュリティ人材フレームワーク」を活用し、各責任者・管理者等の具体的な役割や実施すべきタスク、必要な知識・スキルを明確化すること。	1	×

その他の事項におけるガイドラインの改定等について

ISO:27001:2022（JIS Q 27001：2023）改訂の反映

- ISO/IEC 27001が2022年に改訂（JIS Q 27001は2023年に改訂）されている。総務省のガイドラインはISO/IEC27001をベースに作成されてきたことから、改訂内容における**未反映箇所**について今年度のガイドラインの改定の中で取り込む予定。
 - 既にガイドラインに記載されている内容が多いが、**構成管理におけるドキュメント化、レビュー等の重要性**や、**データマスキング**等に関する記載について検討を行う。
 - ISMS認証取得団体のヒアリング結果から、幹部層との定期的な報告やレビューの重要性とこれらの継続的な実践することにより、組織内にセキュリティの意識が定着しているといった効果がある点を踏まえ、**「リスクベースの運用」、「マネジメントレビュー」、「継続的改善」**という要素（重要インフラ分野における組織統治に関する箇所）をガイドラインに追記を検討する。

幹部層とマネジメント層との関係イメージ

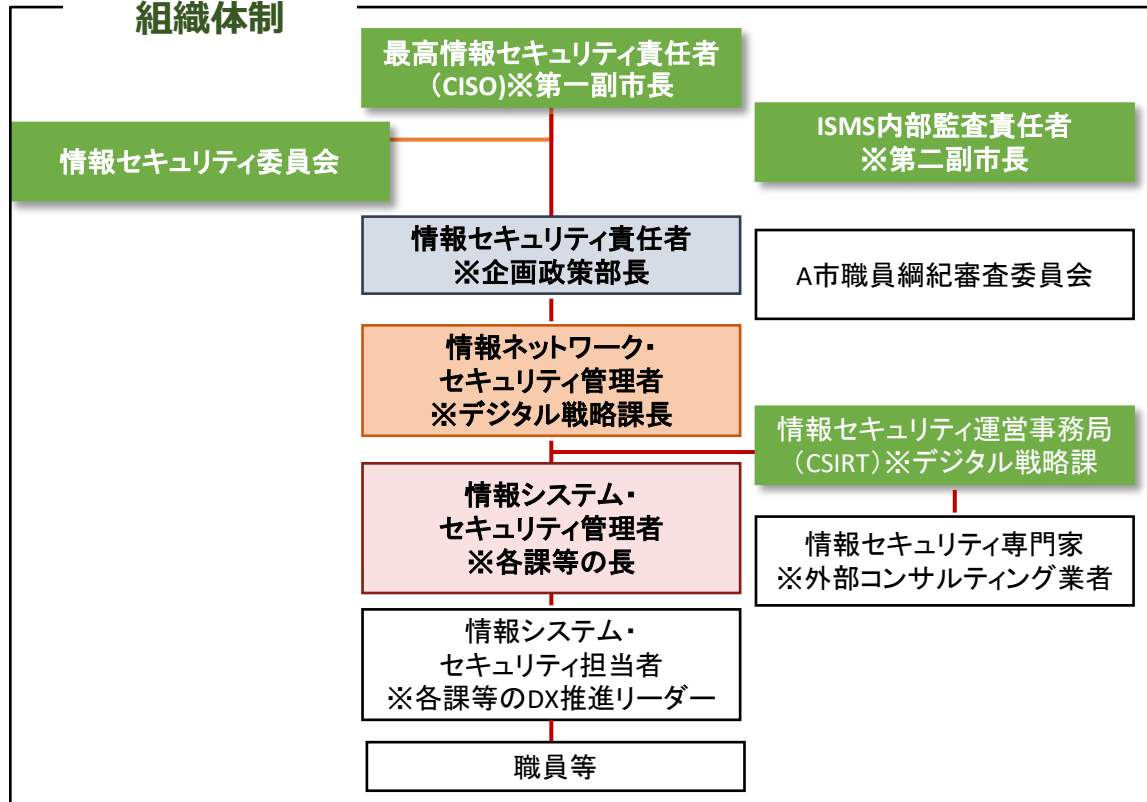


事例 【A市】デジタル戦略課を中心とした全庁統制型ガバナンス

取組

- A市では、副市長をCISO、企画政策部長を情報セキュリティ責任者、デジタル戦略課長を情報ネットワーク・セキュリティ管理者とする体制を構築。
- ISMS認証はデジタル戦略課が取得。情報セキュリティ委員会を年2～3回開催し、**ISMS活動の報告やセキュリティポリシー推進体制、事件事故の事例や動向について共有**を行っている。
- **セキュリティに関する内部監査**はデジタル戦略課が主導し、組織内の**全部署について年1回の自己点検**、一部の部署については**デジタル戦略課職員が訪問し、現地確認**を行っている。

組織体制



成果

デジタル戦略課職員の**情報セキュリティ対策意識の向上**や、PDCAサイクルに基づいた取組みの定着に効果があった。また、ISMS認証取得のための活動から得た知見を、内部監査等を通して庁内全体に展開することで、一定のセキュリティ意識の向上に繋がっていると考えられる。

課題

ガバナンスの実効性はデジタル戦略課による点検に依存する部分が大きく、**デジタル戦略課の負担が大きい**。現状、指摘事項に対する是正状況を確認するフォローアップ体制が整っておらず、是正処置の履行を担保できていないことが課題である。また、**デジタル戦略課以外の部署にいかにして同等のセキュリティ意識の定着を図るかも、検討事項となっている**。

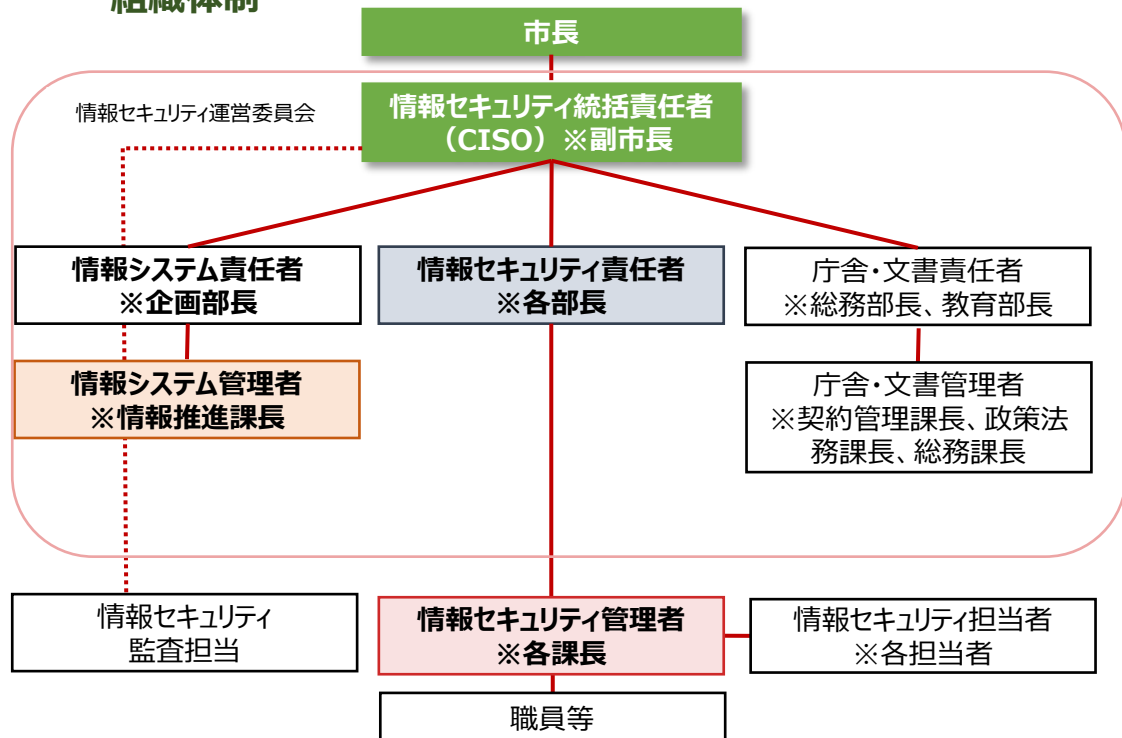
長年の取組みが組織内に定着

事例 【B市】各部・各課に責任を委譲した分散型ガバナンス

取組

- B市ではCISO（副市長）の下、各部長を情報セキュリティ責任者、各課長を情報セキュリティ管理者として位置付けており、各部門に責任を分散した体制を構築している。
- ISMS認証は情報推進課のほか、市民課を始めとした機微情報を取り扱う12課が継続的に取得している。
- 内部監査はISMSを取得している原課同士で相互に行う運用としており、各部署においてISMS認証に基づくセキュリティ対策を行うことが文化として定着している。

組織体制



成果

各部門が情報資産の管理責任を担う仕組みが定着しており、情報部門に依存しない分散型のガバナンスを実現している。また、ISMSの継続運用や相互監査を通じて、各部署のセキュリティ意識や運用レベルの維持向上を図り、原課においてもセキュリティに対する高い意識が醸成されている。

課題

ISMSの維持には継続的な人的・事務的負担が伴い、対象部署が多いことから運用コストも大きい。また、対象課と非対象課との間でセキュリティ意識や取組状況に差が生じるという課題がある。

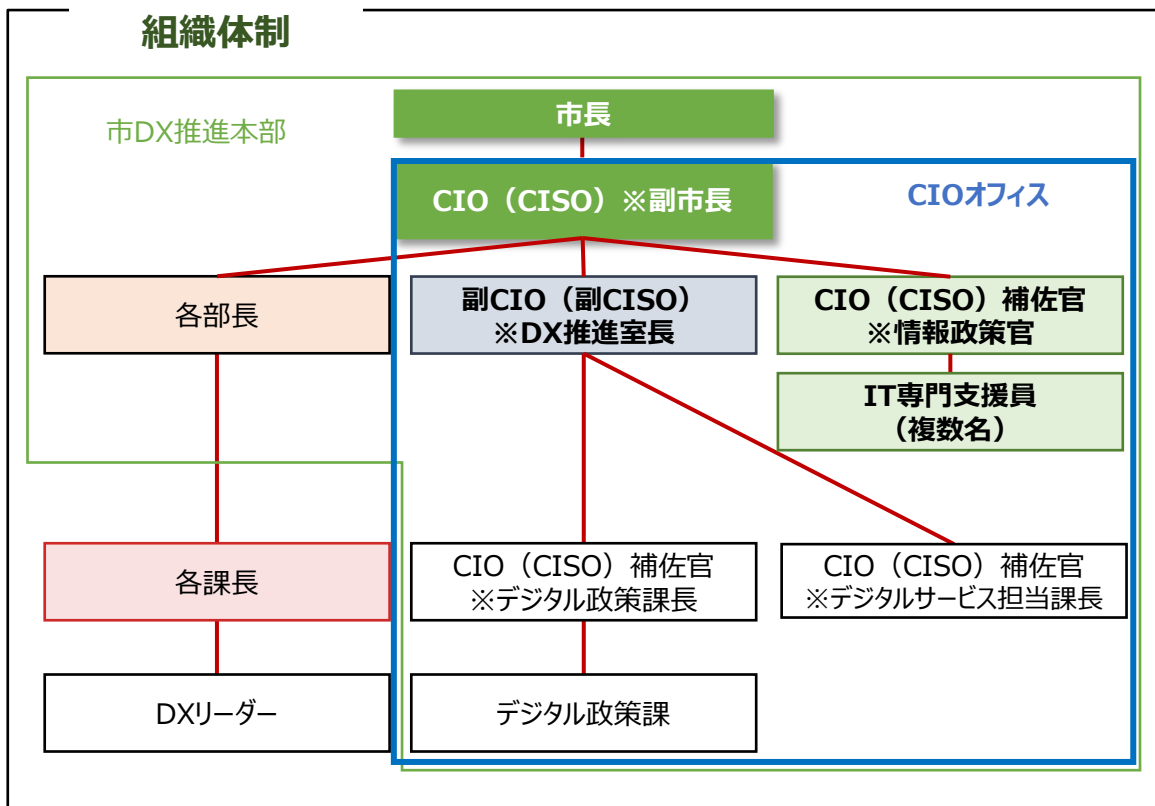
継続することで組織文化へ発展

事例 【C市】「CIOオフィス」によるITガバナンスの推進

取組

- C市では、副市長をCIO（CISO）とし、DX推進室長やデジタル政策課、外部専門人材である情報政策官等から構成される「CIOオフィス」を中心にDX及び情報セキュリティに関するガバナンスを全庁的に推進している。
- 各所管課によるクラウドサービスの利用やシステム導入案件は、全庁的な基準に則り、専門人材であるIT専門支援員の協力のもと、デジタル政策課にて効果・妥当性等を評価している。
- デジタル政策課、および市民サービス担当部門によるISMS認証の取得を継続することで、セキュリティに対する意識が組織に定着している。

組織体制



● 成果

IT調達・構築・運用に関する基準に沿ったシステム導入を行うため「CIOオフィス」を配置し、全庁的なITガバナンスを実践している。専門人材を複数名採用し各部門に対する助言等の支援を行うことで、各所管課が組織の基準に逸脱したシステムを導入することを防止するとともに、**セキュリティに限らず情報システムにおける全体の最適化を目指すことが共通の意識として組織内に浸透**している。

● 課題

ISMS認証を維持するには、内部監査の継続的な実施が必要であり、**職員の負担が伴う**。このため、組織内部から認証継続の必要性を問われる場合がある。また、サイバー攻撃を想定した**ICT-BCPの整備**や緊急時対応計画との整合等が今後の検討課題である。

ITガバナンスを継続的に実践

第4編 地方公共団体におけるクラウド利用等に関する特則（例文・解説）について

- 標準準拠システムの移行を踏まえ、クラウドサービス上で業務システムを利用する場合には、クラウドサービスの特性を踏まえた情報セキュリティ対策を考慮する必要があることから、令和4年度の改定において「**第4編**」を**地方公共団体におけるクラウド利用等に関する特則（例文・解説）**として定めた。
- 標準準拠システムの移行・運用が本格化しているため、これまで「第4編」に示した対策基準の内容を第2編及び第3編における対策基準（例文・解説）とすることで、**クラウドサービスの利用を前提としたセキュリティ対策を周知・徹底をはかる**。

ガイドラインを5編構成 から4編構成に変更する

（クラウドに関する対策基準を第2編及び第3編に移行し、参照を一元化する。）

現行のガイドライン構成

第1編	総則・マネジメントプロセス
第2編	基本方針・対策基準（例文）
第3編	基本方針・対策基準（解説）
第4編	クラウド利用等に関する特則
第5編	付録（権限・責任等の一覧）



ガイドライン改定（案）：3編構成

第1編	総則・マネジメントプロセス
第2編	基本方針（例文） 対策基準（例文） 第4編の対策基準を移行
第3編	基本方針（解説） 対策基準（解説） 第4編の対策基準を移行
第4編	付録（権限・責任等の一覧）

クラウドサービスの利用を前提とした
対策基準とする

情報資産の分類における機密性分類の記載について

■令和6年度の改定において、機密性分類の見直しを行い、「自治体機密性3 A、自治体機密性3 B、自治体機密性3 C、自治体機密性2、自治体機密性1」という5分類となった。

■マイナンバー利用事務系で扱う情報資産については、主に自治体機密性3 Bにあたるが、以下の表においてパブリッククラウド上のサービスはISMAPは利用可とあり、マイナンバー利用事務系にかかる規定（専用回線での接続、インターネットとの分離）と関係がわかりづらく、地方公共団体からの問い合わせが多い状況である。そのため、ガイドラインの記載を分かり易く見直すのはいかがか。

分類	分類基準	情報資産	パブリッククラウドサービス（※1）の範囲
自治体機密性3 A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成23年4月1日内閣総理大臣決定）に定める秘密文書に相当する文書	<例> ・「行政文書の管理に関するガイドライン」上の極秘文書、秘密文書に相当する文書（統一基準における機密性3情報に相当する情報） ・極秘文書：秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書 ・秘密文書：極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、インターネットに接続していない電子計算機又は媒体等に保存することが求められている（※2））
自治体機密性3 B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	<例> ・データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報 （住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	ISMAP登録サービスは利用可（8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要） ※統一基準改定に合わせて、8.3でクラウドサービスの利用について規定
自治体機密性3 C	行政事務で取り扱う情報資産のうち、自治体機密性3 B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	<例> ・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体機密性2	行政事務で取り扱う情報資産のうち、自治体機密性3に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	<例> ・政策検討に関する情報	可 （8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要）
自治体機密性1	自治体機密性2又は機密性3の情報資産以外の情報資産	<例> ・将来公表する予定の文書（白書の案等） ・公表された情報	可

自治体機密性3Bの中でマイナンバー利用事務系における情報資産は、対策基準.3（1）のマイナンバー利用事務系の規定も係るが言及されていない

マイナンバー利用事務系における情報資産についてのデータの利用または保存領域は、インターネットと分離された領域であることを追記

※ 今後、実運用のために記載を明確化する予定。

注）自治体機密性3 C情報については、情報資産単位でのアクセス制御、業務システムログ管理の実施等、βモデルにおいてインターネット接続系に求められている対策を実施することで、インターネット接続系における取扱いが可能。

※1 クラウド事業者が提供するサーバやネットワークなどのインフラを、仮想化技術により複数のユーザで共用し、個々のユーザが、システムの運用体系を完全に制御することが難しいサービスを想定している。

※2 「行政文書の管理に関するガイドライン」（平成23年4月1日内閣総理大臣決定 令和7年2月14日一部改正）第10 秘密文書の管理

図表 22 機密性の分類、分類基準の例示