ISMAP管理基準の改定について

令和６年７月１日
NISC、デジタル庁、総務省、経済産業省

ISMAP管理基準の改定について

- 「政府機関等のサイバーセキュリティ対策のための統一基準群」が令和５年７月（令和５年度版）に改定されたことを踏まえ、改定内容からISMAP管理基準へ取り込むべき内容を整理。
- 整理した内容を反映し、令和６年７月１日にISMAP管理基準を改定。
  【改定内容】新設：４件、既存（例示追加）：４件、既存（文言修正）：１件

〔ISMAP管理基準改定項目〕

項目	変更種別	概要	詳細管理策
1	新設	事業者責任による暗号化消去を新設。	8.1.5.4.P
2	新設	ある情報システムで発生したインシデントが、他の情報システムでも発生する可能性を検討すること（横展開調査）を新設。	16.1.5.10
3	新設	送信側・受信側共に、送信ドメイン認証技術(DMARCやSPF等)による対策を新設。	13.2.3.7.P
4	新設	機械学習方式又はサンドボックス型の不正対策プログラム等の感染リスクの低減手段を新設。	12.2.1.15
5	例示追加	例示として、多要素認証機能の追加。	9.2.3.11.PB
6	例示追加	例示として、手順書確認訓練又はシナリオ非提示型訓練を追加。	7.2.2.18
7	例示追加	例示として、必要に応じてネットワークを幾つかのネットワーク領域に分離する例に必要な単位でセグメントを分離することを追加。	13.1.3.1
8	例示追加	例示として、外部からの不正アクセスによる被害を防止する対策としてWAF等の対策を追加。	13.1.3.5
9	文言修正	統一基準の表現変更に合わせ、ゼロトラストアーキテクチャ（動的なアクセス制御）に修正。	9.1.1.16

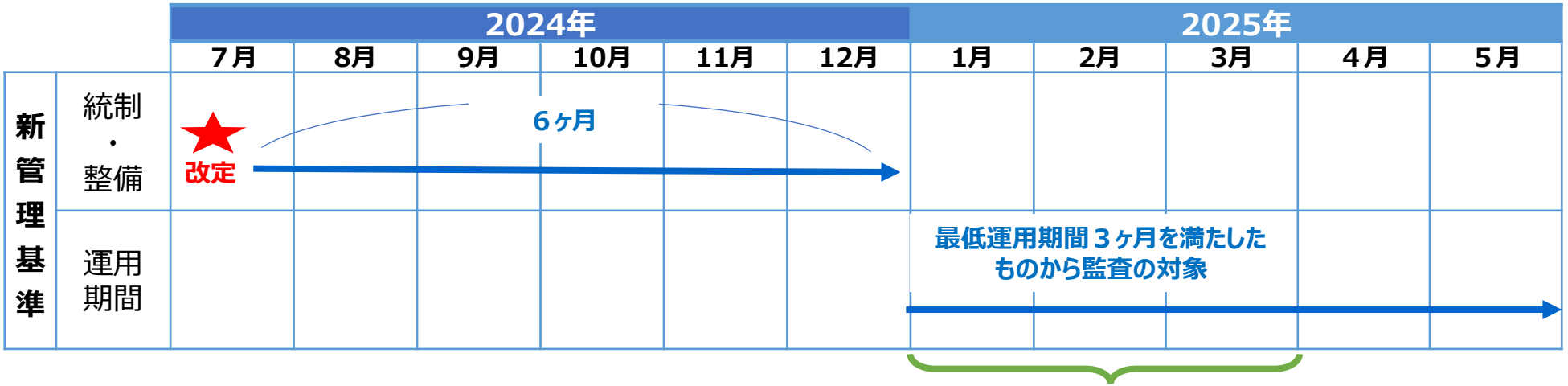
※　実際の詳細管理策の内容等は、「ISMAP管理基準 マニュアル（３章～18章）」をご確認下さい。以下リンク先の最下部にございます「管理基準の配布請求フォーム」より、入手可能です。

https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010028

新管理基準への適応について

- 改定後のISMAP管理基準の適用については、**①2025年1月～3月の3か月間を監査対象期間として含む申請**、または、**②監査対象期間の始期が2025年1月以降の申請**、とする。なお、意欲ある事業者のため、先行適用可能とする。

（参考）管理基準改定後のスケジュールと適用イメージ



パターン	…	2024年12月	2025年1月	2025年2月	2025年3月	2025年4月	…	改正後のISMAP管理基準適用の要否
①			監査対象期間					必要
ー			監査対象期間					不要
②				監査対象期間				必要

監査対象期間の末日が2025年３月末以降の申請から適用

（参考）改定後の管理基準に対するご質問と回答（１/2）

No.	概要	いただいたご質問	回答
1	基準の改定後の適用日について	・改定内容のうち「新設」とされた４項目について、いつまでに完了している必要があるか（＝「詳細管理策に対応する個別管理策が整備されていない」と判断されるタイミング） なお同ページの「2024年7月を基準とし、多要素認証に関する統制整備に６ヶ月、運用期間に３ヶ月の期間を要することから」との記載を根拠として、「2024年12月31日までに整備が完了していれば良い」と解しておりますが、相違ないでしょうか。	ご認識の通り、監査対象期間に2025年１月～３月が含まれるものになりますので、2024年12月までに整備が完了していれば問題ございません。
2	例示追加の管理策について	(例えば・・・)と記載されているところはあくまで例示であり、何らかの対策を実施していれば問題無いという理解で問題無いでしょうか。	ご認識の通り、例示になりますので別の手段での達成も問題ないと考えております。
3	暗号化消去について	暗号化消去については管理策（選択肢）のひとつだという説明がありましたが、復元できない形での消去が出来ていれば暗号化消去でなくとも問題無いという理解で良いのでしょうか。	ご認識の通り、別の手段で達成している場合に非採用を選択されることは十分考えられます。例えば、事業者の責任で除去するものがない場合（利用者鍵管理の管理策のみで契約に関わるお客様関連のデータ消去が達成できている場合等）が考えられます。
4	横展開調査について	16.1.5.10の、横展開調査は具体的にどのような範囲まで必要なのかお教えください。	言明対象範囲内の別のサブサービスや機能・システムの動作箇所を意図しております。インシデントがAPIやプログラムの不具合等に起因した場合に、他の言明対象範囲内でも同様の事象が発生していないか調査いただく等になるかと思います。

（参考）改定後の管理基準に対するご質問と回答（2/2）

No.	概要	いただいたご質問	回答
5	DMARC等の対策について	電子メール・電子的メッセージ通信サービスを提供している事業者だけが対象になるという理解で問題ないでしょうか？また、「電子メール・電子的メッセージ通信サービス」の対象範囲は具体的にどこまでなのかお教えください。	・ メールサーバ（SMTP）、DNSを**機能**として提供しているサービスだけでなく、サービスの一部にメール送信機能を付しているもので、メール送信のFromを政府機関等利用者のドメインに変更できるものも対象に含まれます。 ・ 上記の場合、利用者組織のメールサーバー等に設定するためのDMARCやSPFレコード等に関するパラメーター等の情報を公開されている事業者様も多いかと思われ、本管理策が選択の対象になると考えております。
6	多要素認証について	「その手段として、例えば、クラウドサービス事業者は、多要素認証機能を提供する。」と記載されていますがここは多要素認証機能が必要という理解で問題ないでしょうか。	例えばとありますので、あくまで例示になります。 統一基準群の多要素認証は定義も広いため、強固な認証の大部分があてはまる可能性もございますが、他で強固な認証を実現できている場合はその限りではございません。 ※統一基準上は以下から２つを組みあわせることとなっております。 **知識**（パスワード等、利用者本人のみが知り得る情報）による認証 **所有**（電子証明書を格納するICカード、ワンタイムパスワード生成器、利用者本人のみが所有する機器等）による認証 **生体**（指紋や静脈等、本人の生体的な特徴）による認証