資料３

政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子）

資料３－１　政府機関等の情報セキュリティ対策のための統一基準群の見直しについて（骨子）

資料３－２　統一基準群改定の方向性について

政府機関等の情報セキュリティ対策のための統一基準群の見直しについて（骨子）

資料３－１

１．クラウドサービスの利用拡大を見据えた記載の充実

- 政府情報システムのためのセキュリティ評価制度（ISMAP）の管理基準も踏まえ、クラウドサービス利用者側として実施すべき対策や考え方に係る記載を追加。
  ⇒外部サービスを安全に利用するために、業務内容や取り扱う情報の格付や取扱制限に応じた情報セキュリティ対策を自ら講じられることが重要。

２．情報セキュリティ対策の動向を踏まえた記載の充実

- 政府機関等を標的とした主要なサイバー攻撃や近年の情報セキュリティインシデント事例、最新のセキュリティ対策などを踏まえた記載、また今後取り組むべき情報セキュリティ対策の将来像について記載。
  ⇒従来からの境界型防御を補完するものとして「常時アクセス判断・許可アーキテクチャ」にも目を向ける。また、情報システムの「常時システム診断・対処」を引き続き推進するなど、情報セキュリティ対策基盤を着実に進化させることが重要。

３．多様な働き方を前提とした情報セキュリティ対策の整理

- 新型コロナウイルス感染症対策として政府機関等においても急速に広まったテレワークや遠隔会議の経験も踏まえ、係る多様な働き方を前提とする場合に必要な情報セキュリティ対策について、参照すべき統一基準上の規定や解説を整理することで、政府機関等が実施すべき対策の水準を明確にする。
  ⇒危機管理や働き方改革への対応として、通常とは異なる環境下においても必要な情報セキュリティ水準を確保した上で業務の円滑な継続を図ることが重要。

資料３－２

統一基準群改定の方向性について

１．現状認識と改定の必要性

（１）政府機関等におけるクラウドサービス利用の進展

・デジタル・ガバメント実行計画（令和元年 12 月 20 日改定（閣議決定）。以下「デジガバ実行計画」という。）においても行政機関におけるクラウドサービス利用の徹底の方針が示されるなど、今後クラウド・バイ・デフォルト原則に則った政府情報システムの整備が一層進展するものと認識。

・クラウドサービスの利用に際しては、従来のオンプレミスでの情報システム構築とは異なる特徴として、クラウドサービス提供者側とクラウドサービス利用者側それぞれの責任範囲における情報セキュリティ対策を、各々が実施することにより情報システム全体の情報セキュリティ水準が保たれることに留意が必要。

・クラウドサービス提供者側の情報セキュリティ対策を評価する制度として、「政府情報システムのためのセキュリティ評価制度（ISMAP）」が本年５月に運用を開始したことも踏まえ、統一基準群においてクラウドサービス利用者側に求められる情報セキュリティ対策について記載を充実させることで、クラウドサービス利用時の情報セキュリティ対策のベースラインをより分かりやすく示すことは有用。

・また、政府機関等において情報セキュリティ対策を推進する部門との意見交換等を通じて得られた知見から、クラウドサービスの利用に関連する課題として挙げられる、約款による外部サービスの考え方・捉え方についても、改めて整理することも必要。

（２）サイバー攻撃及び情報セキュリティ対策の動向

・前回の統一基準群改定以降、政府機関等においてはサイバー攻撃による大規模なインシデントの発生は認知されていないものの、引き続き標的型攻撃をはじめとする高度なサイバー攻撃への備えは重要。情報システムの監視や可視化といった対策が一般的なものになりつつある状況等も踏まえ、政府機関等へのこれら対策の導入の検討に資するべく記載の充実を図ることは有用。その他、統一基準群に記載の対策について、情報セキュリティインシデント事例や最新の考え方等を踏まえた所要の修正を行うことも必要。

（３）多様な働き方を前提とした情報セキュリティ対策

・今般の新型コロナウイルス感染症への対策として政府機関等においてもテレワークや遠隔会議の実施等が必要となる状況が発生しているが、係る緊急対応としてだけでなく、今後はこうした多様な働き方の定着により政府機関等の施設外での業務実施機会や政府機関等が外部サービスを利用して他の組織と連携する機会が増えるものと認識。

・そのような多様な働き方を前提とした情報セキュリティ対策は必ずしも従来からの対策と異なるものではないが、特有の留意点や考え方等を示すことは、各政府機関等におい

て対策を検討する上で有用。

（４）その他所要の修正

・前回の統一基準群改定（平成 30 年７月）以降、サイバーセキュリティ基本法に基づく監査の結果及び政府機関等から寄せられた意見等を踏まえた修正や、統一基準群と関連している文書・マニュアル類との関係を再整理することで、政府機関等における情報セキュリティ対策の運用の円滑化に寄与。

２．次期改定により実現を目指す情報セキュリティ対策の在り方

・現状認識と改定の必要性及び政府機関等が目指すべき情報セキュリティ対策の将来像を踏まえ、次期改定では政府機関等における情報セキュリティ対策の在り方として、以下を目指す。

（１）政府機関等がクラウドサービスに代表される外部サービスを安全に利用するために、業務内容や取り扱う情報の格付や取扱制限に応じた情報セキュリティ対策を自ら講じられること。

（２）情報セキュリティ対策の防護壁の脆弱性を狙った複雑・巧妙なサイバー攻撃への対応として、重厚な防護壁を構築するだけではなく、常時アクセス判断・許可アーキテクチャの導入も視野に入れ、情報システムの常時システム診断・対処を引き続き推進するなど、政府機関等全体として必要な情報セキュリティ対策の基盤を着実に進化させること。

（３）危機管理や働き方改革への対応として、通常とは異なる環境下においても必要な情報セキュリティ水準を確保した上で事業を継続できること。

３．改定のコンセプト

（１）クラウドサービスの利用拡大を見据えた記載の充実

①クラウドサービスの利用者側として実施すべき対策や考え方に係る記載の追加

- 現行版（平成 30 年度版）統一基準にて規定されているクラウドサービスの利用に係る対策は、主として情報システムの企画、要件定義から調達段階までを対象としたものであるところ、情報システムのライフサイクルにおける構築、運用・保守、更改・廃棄の各段階についても、クラウドサービス利用者側として特に気を付けるべき対策や考え方等について、国際標準である ISO/IEC 27017:2015 のクラウドサービスカスタマに向けた実施手引き等を参考に記載を追加することにより、政府機関等におけるクラウドサービス利用における情報セキュリティのベースラインを示す。また、近年発生したクラウドサービス利用における重大インシデントを踏まえた対策を追加。

②政府情報システムのためのセキュリティ評価制度（ISMAP）を踏まえた記載の追加

- 政府機関等における、ISMAP を活用したクラウドサービス利用に係る記載を追加。

③約款による外部サービスに係る考え方の再整理

- 約款による外部サービスとクラウドサービスは、現実的には区別が容易ではない場合もあると承知しているところ、それぞれの規定が異なるタイミングで統一基準へ追加された（約款による外部サービスは平成 26 年版、クラウドサービスは平成 28 年度版。）ことから両者を別個のものとして扱う構成になっていることは、政府機関等の情報セキュリティ運用の現場での負担となっているものと認識。
- 約款による外部サービスに係る規定が追加された趣旨には、シャドーＩＴ（職員等による、所属組織の把握しない情報サービスの利用）の抑止が含まれ、運用上も最初から両者を区別して対策を実施するのではなく、利用を検討するサービスについて、政府機関等自らが開発し、又は専用に構築されたサービスではない汎用的な外部サービスの利用であることを踏まえたリスク評価等をまず行った上で、当該サービスの業務利用の可否や取扱うことのできる情報等を組織として判断することが望ましいと思料されるところ、クラウドサービスに係る規定との構成見直しや用語の再定義などを含む所要の改定を行う。

（２）情報セキュリティ対策の動向を踏まえた記載の充実

①政府機関等に対する主要なサイバー攻撃への対策に係る記載の充実

- DDoS 攻撃、標的型攻撃への対策について、近年の動向を踏まえた解説を追加。
- EDR（Endpoint Detection and Response）ソフトウェアの導入及び同ソフトウェア等により検知される脅威の監視・分析に係る運用等、サイバー攻撃を受けることを前提としたエンドポイントセキュリティ対策についての解説を追加。
- 前回改定時（平成 30 年度版）に追加した、①未知の不正プログラムに係る被害の未然防止／拡大防止、②IT 資産管理の自動化とそれによる脆弱性への迅速な対応、③事案が発生した際にも被害を無効化する、データ保護による情報漏えい対策の導入をコンセプトとした対策は引き続き推奨すべきものであると認識しているところ、政府機関等における導入の検討に資する解説の追加。

②情報セキュリティインシデント事例を踏まえた記載の追加

- 情報システムの運用終了時における、機器の廃棄やリース契約終了に伴う返却の際の留意点について解説を追加。
- 電磁的記録媒体廃棄時における情報の抹消について、近年政府機関等においても利用が拡大している SSD のデータ消去に係る解説や、暗号化消去（ディスク全体を暗号化し、その復号のための鍵を廃棄することによる論理的削除方法）に係る解説を追加。

③情報セキュリティ対策に係る最新の考え方等の反映

- 十分な強度を持ったパスワードの生成方法については、情報システムの運用方法や認証技術の方式により異なるものであり必ずしも明らかではないところ、政府機関等における指針となるような考え方を解説に追加。

- 電子ファイルの受け渡し方法について、暗号化したファイルを電子メールに添付する場合は、直後にパスワードを電子メールで送付するのではなく、あらかじめ送付先との間でパスワードを電子メールとは別の方法で伝達することについて、より明示的な記載とする。
- 従来からの物理的な境界で情報セキュリティを確保する考え方を補完するものとして、常時アクセス判断・許可アーキテクチャに係る内容を追加。

（３）多様な働き方を前提とした情報セキュリティ対策の整理

- 政府機関等においても、時間や場所に柔軟性を持たせた働き方の拡大が見込まれるところ、自宅もしくは自宅以外のワーキングスペース等でテレワークを行う際の情報セキュリティ対策について、参照すべき統一基準上の規定や解説を整理する。

（４）その他所要の修正

①標準ガイドライン群との整合性の確保

- デジガバ実行計画においても「KPI：標準ガイドライン群と統一基準群等の一層の整合性の確保と融合」と定められているところ、令和２年３月に改定された標準ガイドライン群の内容も踏まえ、用語や組織内に構築すべき体制の位置付け等について一層の整合性を図る。

②理解促進に資する解説等の追加・修正

- 一部の政府機関等において、本来統一基準に定める機密性３情報に該当しない情報を機密性３情報として扱っている事例があると承知しているところ、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）を引用する等、統一基準の格付の定義に解説や例示を追加することで認識の齟齬の解消を図る。
- その他、規定の趣旨等がより明確なものとなるよう、解説を追加するなど所要の改定を行う。

③技術的な修正等

- ガイドラインの解説に含まれる参考資料名や参考 URL 等について、最新の情報に基づいた更新、削除を行う。

④個別マニュアル群の整理

- 現在 NISC ホームページ上で公開している各種マニュアル等には、文書作成当時の統一基準の内容に基づいたまま、その後の統一基準群の改定時に更新されていないものが多数存在している。これら各種マニュアル等について内容を精査し、公開の停止や過去版の統一基準に基づいていることを明記した上で参考資料として公開する等の整理を行う。

以上