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改定（案）について

資料５－１

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。

2. 改定の概要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

«主な内容»

✓ 外部サービスの再定義と取り扱う情報に応じた適切なセキュリティ対策の実施
⇒境目が曖昧となっている「約款による外部サービス」と「クラウドサービス」を「外部サービス」として統合した上で、「外部サービス」上での要機密情報の取り扱いの有無により、求めるセキュリティ対策のレベルを整理。
⇒政府機関等が外部サービスを選択する際には、セキュリティ確保のために必要な事項を十分に考慮した上で、外部サービスが当該セキュリティ要件を満たす（※）ことを確認することが必要。

※民間事業者等が不特定多数の利用者に対して提供するSNS等の、画一的な約款や規約等への同意のみで利用可能となる外部サービス（従来の「約款による外部サービス」）については、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない点は、従前より変更なし。

✓ ISMAP制度の活用
⇒要機密情報を取り扱う外部サービスのうちクラウドサービスを利用する場合に、その選定においてISMAP制度を活用。

✓ 外部サービス利用時のライフサイクルに渡るセキュリティ要件の追加
⇒外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策のみならず、構築・運用・廃棄等のライフサイクルに渡ることから、要機密情報を取り扱う外部サービスの利用における導入・構築・運用・保守・更改・破棄の各フェーズのセキュリティ対策に係る規定を、ISO/IEC27017:2015を参考に追加。

✓ 外部サービスに係るシャドーIT対策
⇒組織の承認を得ずに職員等が外部サービスを利用するシャドーITは監視が不十分になりやすく、セキュリティリスクが高まる等の問題がある。シャドーIT対策として、外部サービス利用時の組織内での承認・審査・申請の手続きを規定。

※従来の統一基準群では「約款による外部サービス」のみを承認等の対象としていたが、クラウドサービスを含む外部サービス全体を対象とした。

2. 改定の概要2

２．情報セキュリティ対策の動向を踏まえた記載の充実

«主な内容»

✓ 政府機関等に対する主要なサイバー攻撃や近年のサイバーセキュリティインシデント事例を踏まえた対策等の記載の追加
⇒以下の解説を追加し、より強固なサイバーセキュリティ対策を例示。

- EDR　端末の動作を監視し、異常時の管理者による迅速な対応を支援するための機能
- CDNサービス　Webコンテンツを複数のサーバに分配配置し、大量アクセスの負荷を軽減するサービス
- IT資産管理ソフトウェア　Windows Updateに代表されるセキュリティ更新ソフトウェアの適用状況を管理し、最適な状態を維持するソフトウェア
- 標的型メール攻撃　組織や個人の情報を入念に調査し情報を収集した上で、攻撃対象が疑念を抱かないよう、巧妙に偽装したメールにより仕掛けてくる攻撃
- 暗号化消去　暗号化された情報を復号するための「鍵」を抹消する論理的削除方法
- SSD等内蔵記録媒体を含む種々の電磁的記録媒体廃棄時の記録された情報の抹消
  フラッシュメモリタイプの電磁的記録媒体は、データ抹消ソフトウェアによる上書きを実施しても、実際には書き込みが行われず、消去すべき情報がそのまま残ってしまう領域が発生してしまうことへの注意

✓ 情報セキュリティ対策に係る最新の考え方等の反映
⇒アクセス制御機能の例として、常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ。「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という性悪説に基づいた考え方。）に関する記載を追加。
⇒メール添付による暗号化された電子ファイル受け渡し時の復号用パスワード受け渡し方法に関する記載を追加。また、暗号化する際に設定するパスワードやパスフレーズに求める十分な長さと複雑さについての解説を追加。

2. 改定の概要3

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

«主な内容»

✓ テレワークに係る項目の新設
⇒テレワークを実施する際のサイバーセキュリティ対策に係る記述が複数の部に分散していたため項目を新設。テレワークに特有の情報セキュリティ対策について包括的に記載。

✓ Web会議サービス利用時の対策に係る項目の新設
⇒政府機関等において利用が急増したWeb会議サービスについて、利用時に行うべき情報セキュリティ対策について、項目を新設して記載。

✓ 機関等支給以外の端末に係る留意事項等の整理
⇒機関等支給以外の端末に係る記述が複数の部に分散していたため項目を新設して記載。
⇒機関等支給以外の端末においては、情報セキュリティ水準を一定以上に保ち続けることが困難であり、情報セキュリティインシデントの引き金となる可能性が高いことから、機関等が支給する端末の利用を原則としつつ、やむを得ず利用する場合の対策について整理。