「政府機関の情報セキュリティ対策のための統一基準群（案）」の概要について

資料2

現行の統一基準群の課題と改定の方向性

◆ 新たな脅威への対応のための基準の追加

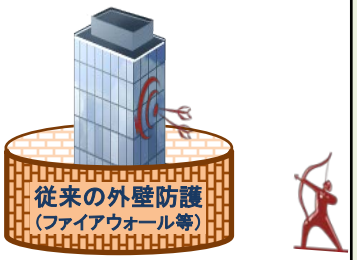
◆ 不明確で分かりにくい基準の明確化

主な改定内容（※）

◆ 標的型攻撃への対策

➢ 標的型攻撃から守るべき重点業務等を特定し、関係する情報システムについて、内部侵入を早期発見し、活動を困難化するための対策を計画的に講ずる。

標的型攻撃のイメージ



・特定の組織の情報に狙い
・従来の外壁防護を無効化

内部対策の強化が重要

◆ サプライチェーン・リスクへの対策

➢ 情報システムの構築等の外部委託の際、委託先における不正機能の混入防止のため、厳正な管理を要求。

◆ 分かりやすく、守られやすい基準

➢ 定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人毎の遵守事項の集約化、形骸化した規定の見直し等により、分かりやすく、守られやすい基準作りを目指す。

（現行の統一基準における規定の例）

行政事務従事者は、障害・事故等の発生を知った場合には、それに関係する者に連絡するとともに、統括情報セキュリティ責任者が定めた報告手順により、障害・事故等に対応する責任者、及び障害・事故等に対応する責任者を通じて最高情報セキュリティ責任者にその旨を報告すること。

ただし、緊急やむを得ない事情により、障害・事故等に対応する責任者に　報告することができない場合は、定められた　報告手順に従って、最高情報セキュリティ責任者に報告すること。

（見直し案）

行政事務従事者は、情報セキュリティインシデントを認知した場合には、各府省庁の報告窓口に速やかに連絡し、指示に従うこと。

（※「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議決定）において決定された事項を踏まえ検討。）