ASP・SaaS における
情報セキュリティ対策ガイドライン

ASP・SaaS の情報セキュリティ対策に関する研究会

平成２０年　１月３０日

目次

Ⅰ　序編

Ⅰ．１　はじめに　1
Ⅰ．２　ASP・SaaS とは　1
Ⅰ．３　ガイドラインの対象範囲　1
Ⅰ．４　ガイドラインの位置付け　2
Ⅰ．５　ガイドライン活用の効果　2
Ⅰ．６　ガイドラインの全体構成　3
Ⅰ．７　ASP・SaaS サービス種別のパターン化　4
　Ⅰ．７．１　パターン化の考え方　4
　Ⅰ．７．２　典型的サービスのパターン分類　6
Ⅰ．８　ガイドラインの利用方法　8
　Ⅰ．８．１　対策項目　8
　Ⅰ．８．２　基本・推奨　8
　Ⅰ．８．３　ベストプラクティス　8
　Ⅰ．８．４　評価項目　8
　Ⅰ．８．５　対策参照値　8
　Ⅰ．８．６　利用手順　9
Ⅰ．９　用語の定義　10
　Ⅰ．９．１　JIS Q 27001 の定義を踏襲している用語　10
　Ⅰ．９．２　本ガイドライン独自に定義する用語　10
Ⅰ．１０　参考文書　12

Ⅱ　組織・運用編

Ⅱ．１　情報セキュリティへの組織的取組の基本方針　13
　Ⅱ．１．１　組織の基本的な方針を定めた文書　13
Ⅱ．２　情報セキュリティのための組織　15
　Ⅱ．２．１　内部組織　15
　Ⅱ．２．２　外部組織（データセンタを含む）　16
Ⅱ．３　連携 ASP・SaaS 事業者に関する管理　17
　Ⅱ．３．１　連携 ASP・SaaS 事業者から組みこむ ASP・SaaS サービスの管理　17
Ⅱ．４　情報資産の管理　18
　Ⅱ．４．１　情報資産に対する責任　18

Ⅱ．４．２　情報の分類　19
Ⅱ．４．３　セキュリティ方針及び要求事項の遵守、点検及び監査　20
Ⅱ．５　従業員に係る情報セキュリティ　21
Ⅱ．５．１　雇用前　21
Ⅱ．５．２　雇用期間中　22
Ⅱ．５．３　雇用の終了又は変更　23
Ⅱ．６　情報セキュリティインシデントの管理　24
Ⅱ．６．１　情報セキュリティインシデント及びぜい弱性の報告　24
Ⅱ．７　コンプライアンス　25
Ⅱ．７．１　法令と規則の遵守　25
Ⅱ．８　ユーザサポートの責任　27
Ⅱ．８．１　利用者への責任　27

Ⅲ　物理的・技術的対策編

Ⅲ．１　アプリケーション、プラットフォーム、ハードウェア、ネットワークに共通する情報セキュリティ対策　28
Ⅲ．１．１　運用管理に関する共通対策　28
Ⅲ．２　アプリケーション、プラットフォーム、ハードウェア、サービスデータ　35
Ⅲ．２．１　アプリケーション、プラットフォーム、ハードウェアの運用・管理　35
Ⅲ．２．２　アプリケーション、プラットフォーム、ハードウェアのセキュリティ対策　41
Ⅲ．２．３　サービスデータの保護　43
Ⅲ．３　ネットワーク　45
Ⅲ．３．１　外部ネットワーク(利用者、管理者、連携 ASP・SaaS 事業者)からの不正アクセス防止　45
Ⅲ．３．２　外部ネットワーク(利用者、管理者、連携 ASP・SaaS 事業者との接続)におけるセキュリティ対策　50
Ⅲ．４　建物、電源(空調等)　53
Ⅲ．４．１　建物の災害対策　53
Ⅲ．４．２　電源・空調の維持と災害対策　54
Ⅲ．４．３　火災、逃雷、静電気からサービス提供用機器を防護するための対策　56
Ⅲ．４．４　建物のセキュリティ対策　58
Ⅲ．５　その他　61
Ⅲ．５．１　機密性・完全性を保持するための対策　61
Ⅲ．５．２　事業者の運用管理端末のセキュリティ　63
Ⅲ．５．３　媒体の保管と廃棄　65

Ⅳ　参考資料

Annex 1　ASP・SaaS サービスの典型的な構成要素と情報資産

Annex 2　組織・運用編　対策項目一覧表

Annex 3　物理的・技術的対策編　対策項目一覧表