「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」改正案の新旧対照表

（傍線部分は改正部分）

○個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
疑義が生じ得る記載の修正

改　正　案	現　行
2-2-1. 個人情報の利用目的関係（法第１５条～１６条関連）	**2-2-1. 個人情報の利用目的関係（法第１５条～１６条関連）**
（略）	（略）
（５）適用除外（法第１６条第３項関連）	（５）適用除外（法第１６条第３項関連）
（略）	（略）
（ⅲ）公衆衛生の向上等（法第１６条第３項第３号関連）	（ⅲ）公衆衛生の向上等（法第１６条第３項第３号関連）
法第１６条第３項第３号 （略）	法第１６条第３項第３号 （略）
公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）は、その適用を受けない。	公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により、公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）は、その適用を受けない。
事例１）健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究又は統計調査のために、個人名を伏せて研究者等に提供する場合	事例１）健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究又は統計調査のために、個人名を伏せて研究者等に提供する場合
事例２）不登校や不良行為等について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合	事例２）不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

技術的安全管理措置に情報システムのぜい弱性を突いた攻撃への対策及びその例示の追加

改　正　案	現　行
2-2-3-2. 安全管理措置（法第２０条関連） 法第２０条 （略） （略） 技術的安全管理措置 技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。 【技術的安全管理措置として講じなければならない事項】 ①個人データへのアクセスにおける識別と認証 ②個人データへのアクセス制御 ③個人データへのアクセス権限の管理 ④個人データのアクセスの記録 ⑤個人データを取り扱う情報システムについての不正ソフトウェア対策 ⑥個人データの移送・送信時の対策 ⑦個人データを取り扱う情報システムの動作確認時の対策 ⑧個人データを取り扱う情報システムの監視 ⑨個人データを取り扱う情報システムのぜい弱性を突いた攻撃への対策 【各項目を実践するために講じることが望まれる手法の例示】 ※技術的安全管理措置については、①から⑨までの各項目を遵守するとともに、複数の手法を組み合わせ、個人データ及びそれを取り扱う情報システム全体の安全性を確保することが重要である。各項目を実践するための各手法については、以降の①～⑨において、項目	**2-2-3-2. 安全管理措置（法第２０条関連）** 法第２０条 （略） （略） 技術的安全管理措置 技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。 【技術的安全管理措置として講じなければならない事項】 ①個人データへのアクセスにおける識別と認証 ②個人データへのアクセス制御 ③個人データへのアクセス権限の管理 ④個人データのアクセスの記録 ⑤個人データを取り扱う情報システムについての不正ソフトウェア対策 ⑥個人データの移送・送信時の対策 ⑦個人データを取り扱う情報システムの動作確認時の対策 ⑧個人データを取り扱う情報システムの監視 【各項目を実践するために講じることが望まれる手法の例示】 ※技術的安全管理措置については、①から⑧までの各項目を遵守するとともに、複数の手法を組み合わせ、個人データ及びそれを取り扱う情報システム全体の安全性を確保することが重要である。各項目を実践するための各手法については、以降の①～⑧において、項目

ごとに例示する。また、技術的安全管理措置の典型的な手法には例えば次のような方法がある。	ごとに例示する。また、技術的安全管理措置の典型的な手法には例えば次のような方法がある。
（略）	（略）
⑨「個人データを取り扱う情報システムのぜい弱性を突いた攻撃への対策」を実践するために講じることが望まれる手法の例示 ・ウェブアプリケーションやシステム基盤（ＯＳやミドルウェア等）に対してぜい弱性診断（例えば、ウェブアプリケーション診断、プラットフォーム診断等）を実施し、検出されたぜい弱性に対処 ※攻撃手法は日々変化するため、定期的にぜい弱性診断を実施することが望ましい。 ・ウェブアプリケーションのぜい弱性を突いた攻撃からの保護（例えば、クラウドＷＡＦ（ウェブアプリケーションファイアウォール）の活用等） ・ぜい弱性を作り込まない設計、コーディングの実施の活用	（追加）
（略）	（略）
2-2-3-4. 委託先の監督（法第２２条関連）	**2-2-3-4. 委託先の監督（法第２２条関連）**
法第２２条 （略）	法第２２条 （略）
（略）	（略）
①委託先の選定	①委託先の選定
（略）	（略）
（エ）技術的安全管理措置 ・ 個人データへのアクセスにおける識別と認証 ・ 個人データへのアクセス制御 ・ 個人データへのアクセス権限の管理	（エ）技術的安全管理措置 ・ 個人データへのアクセスにおける識別と認証 ・ 個人データへのアクセス制御 ・ 個人データへのアクセス権限の管理

・ 個人データのアクセスの記録 ・ 個人データを取り扱う情報システムについての不正ソフトウェア対策 ・ 個人データの移送・送信時の対策 ・ 個人データを取り扱う情報システムの動作確認時の対策 ・ 個人データを取り扱う情報システムの監視 ・ 個人データを取り扱う情報システムのぜい弱性を突いた攻撃への対策 （略）	・ 個人データのアクセスの記録 ・ 個人データを取り扱う情報システムについての不正ソフトウェア対策 ・ 個人データの移送・送信時の対策 ・ 個人データを取り扱う情報システムの動作確認時の対策 ・ 個人データを取り扱う情報システムの監視 （略）
５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・ 規格 （１）個人情報保護のためのマネジメント体制の確立 個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのマネジメントシステムを確立し、実施し、維持し及び改善を行うことが望ましい。 なお、その体制の整備に当たっては、日本工業規格 JIS Q 15001「個人情報保護マネジメントシステム－要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 JIS X 5070「セキュリティ技術－情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム―要求事項」、日本工業規格 JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」、独立行政法人情報処理推進機構（ＩＰＡ）の「組織における内部不正防止ガイドライン」・「安全なウェブサイトの作り方」、総務省・経済産業省の「電子政府における調達のために参照すべき暗号のリスト （ＣＲＹＰＴＲＥＣ暗号リスト）」・「IoT セキュリティガイドライン」、ISO/IEC 18033（暗号アルゴリズム国際規格）等を、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができる。 （略）	**５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・ 規格** （１）個人情報保護のためのマネジメント体制の確立 個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのマネジメントシステムを確立し、実施し、維持し及び改善を行うことが望ましい。 なお、その体制の整備に当たっては、日本工業規格 JIS Q 15001「個人情報保護マネジメントシステム－要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 JIS X 5070「セキュリティ技術－情報技術セキュリティの評価基準」、日本工業規格 JIS Q 27001「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム―要求事項」、日本工業規格 JIS Q 27002「情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」、独立行政法人情報処理推進機構（ＩＰＡ）の「組織における内部不正防止ガイドライン」、総務省・経済産業省の「電子政府における調達のために参照すべき暗号のリスト （ＣＲＹＰＴＲＥＣ暗号リスト）」、ISO/IEC 18033（暗号アルゴリズム国際規格）等を、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にすることができる。 （略）