

WebMiCS 文書体系サンプル「情報セキュリティ〔2〕」を追加しました

2024 年 7 月 1 日

いつも WebMiCS コースをご利用いただきまして、誠にありがとうございます。

この度、WebMiCS に新しい文書体系サンプル「情報セキュリティ〔2〕」を追加しましたので、お知らせいたします。

対象のお客様

WebMiCS コースをご利用中のお客様

「情報セキュリティ〔2〕」のご利用方法

WebMiCS の [管理者機能] > [サンプル取り込み] > [文書体系サンプル] > 「情報セキュリティ〔2〕(サンプル)」からダウンロードできます。

「情報セキュリティ〔2〕」の詳細

文書体系サンプルの詳細につきましては、既存の文書体系サンプル「情報セキュリティ〔1〕」から「情報セキュリティ〔2〕」への変更点を、次ページ以降に記載しておりますので、ご確認ください。

Q & A

- Q.** 当社は文書体系サンプル「情報セキュリティ〔1〕」を利用しています。その場合、「情報セキュリティ〔2〕」に移行しなければならないのでしょうか？
- A.** 既に運用しているものから移行する必要はございません。
ただし、「情報セキュリティ〔2〕」は「情報セキュリティ〔1〕」よりも文書体系をシンプルにしており、さらに、追補版である ISO/IEC 27001:2022/Amd. 1:2024 に対応しております。
「情報セキュリティ〔2〕」をご覧いただき、使いやすいと判断された場合には、新しい文書体系サンプルに移行したり、変更点を現在運用中のものに反映する等、ご活用いただきたく存じます。

文書サンプルの重要な修正

こちらでは、後述する「情報セキュリティ〔1〕」から「情報セキュリティ〔2〕」への変更点のうち、2024年2月発行のISO/IEC 27001:2022/Amd. 1:2024にて追加された気候変動対応の要求事項に関する変更について、抜粋してご紹介します。

引き続き「情報セキュリティ〔1〕」をご利用される場合は、各修正点に記載している「情報セキュリティ〔1〕」への反映方法の一例をご確認ください。

『情報セキュリティマニュアル』

「2.1 適用規格」の追加

適用規格であるISO/IEC 27001が明示されるように変更しました。

また、2024年2月に発表されたISO/IEC 27001:2022/Amd. 1:2024にて追加された気候変動対応の要求事項に関する反映されていることが明示的になるように変更いたしました。

「情報セキュリティ〔1〕」への反映方法の一例

- (1) 「2 引用規格」を「2 適用規格」に変更
- (2) 「2 適用規格」の内容を以下に変更

2.1 適用規格

JIS Q 27001:2023 (ISO/IEC 27001:2022/Amd.1:2024) 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項

2.2 引用規格

JIS Q 27000:2019 (ISO/IEC 27000:2018) 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-用語

- (3) 目次を更新

「4.1 当社及びその状況の理解」

ISO/IEC 27001:2022/Amd. 1:2024にて追加された気候変動対応の要求事項に関する変更を加えました。

「情報セキュリティ〔1〕」への反映方法の一例

- (1) 「4.1 当社及びその状況の理解」の枠線で囲われた内容を以下に変更。

当社は、組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を決定する。

その際、気候変動が関連する課題かどうかを決定する。

「4.2 利害関係者のニーズ及び期待の理解」

ISO/IEC 27001:2022/Amd. 1:2024 にて追加された気候変動対応の要求事項に関する変更を加えました。

「情報セキュリティ〔1〕」への反映方法の一例

(1) 「4.2 利害関係者のニーズ及び期待の理解」の枠線で囲われた内容を以下に変更。

組織は、次の事項を決定しなければならない。

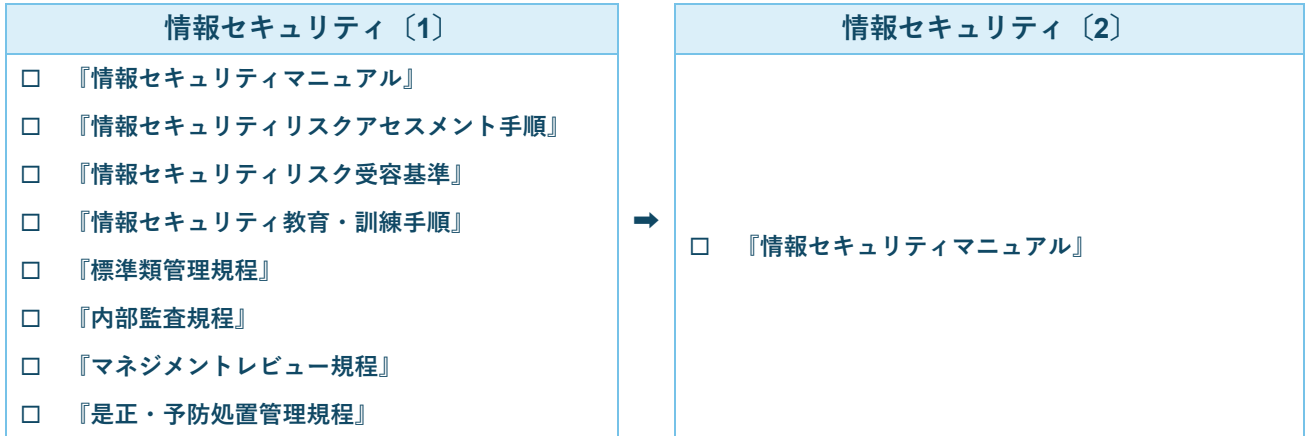
- a) ISMS に関連する利害関係者
- b) それらの利害関係者の、関連する要求事項 **(気候変動に関するものも含む)**
- c) それらの要求事項のうち、ISMS を通して取り組むもの

「情報セキュリティ〔1〕」から「情報セキュリティ〔2〕」への変更点

文書体系の構成変更 及び 内容の改善について示します。

規程類の統合・内容改善

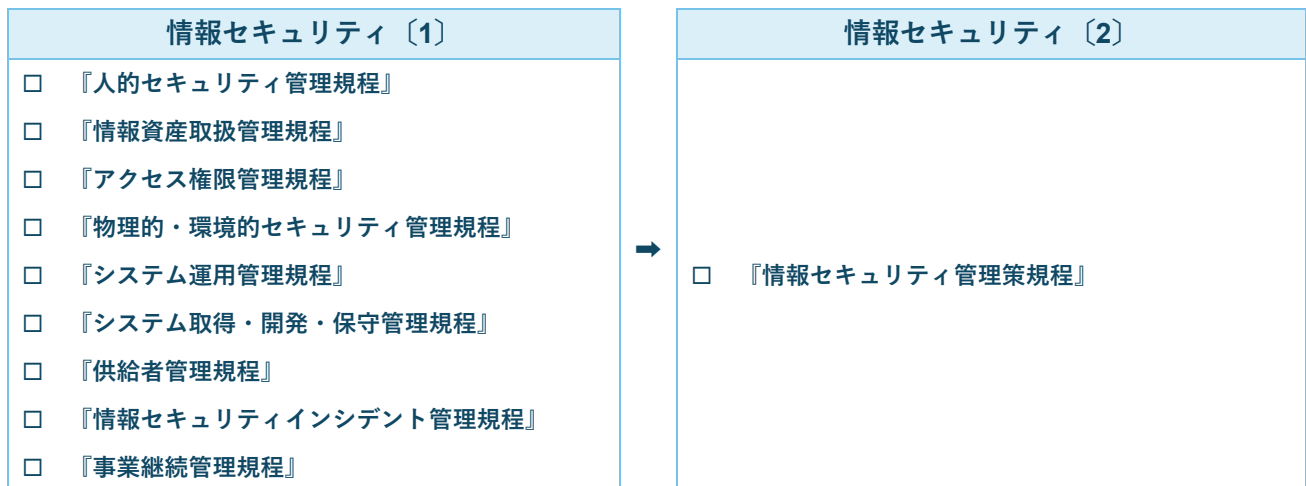
規程類を『情報セキュリティマニュアル』及び『情報セキュリティ管理策規程』に統合しました。



【変更点】

- 「1 適用範囲」
 - 「事業所の適用範囲」を「物理的適用範囲」に呼称を変更。
 - 「組織的適用範囲」及び「インターフェースと依存関係」を追加。
- 「2 適用規格」
 - 章タイトルを「2 引用規格」から「2 適用規格」へ変更し、「2.1 適用規格」と「2.2 引用規格」からなる構成へ変更。
 - 「2.1 適用規格」に適用規格である ISO/IEC 27001 が明示されるように変更。
 - 2024 年 2 月に発表された ISO/IEC 27001:2022/Amd. 1:2024 にて追加された気候変動対応の要求事項に関しても反映されていることが明示的になるように変更。
- 「4.1 当社及びその状況の理解」
 - ISO/IEC 27001:2022/Amd. 1:2024 にて追加された気候変動対応の要求事項に関する記載を追加。
 - 新規帳票『組織状況管理表』を参照する形に変更。
- 「4.2 利害関係者のニーズ及び期待の理解」
 - ISO/IEC 27001:2022/Amd. 1:2024 にて追加された気候変動対応の要求事項に関する記載を追加。
 - 新規帳票『組織状況管理表』を参照する形に変更。
- 「5.3 組織の役割、責任及び権限」
 - 帳票『組織の役割・責務一覧』を参照する形に変更。

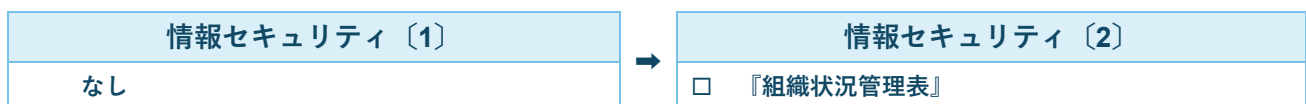
- 「6.1.2 情報セキュリティリスクアセスメント」
 - 『情報セキュリティリスクアセスメント手順』及び『情報セキュリティリスク受容基準』の内容を統合。
 - 『情報資産リスクアセスメント表』を参照するように修正。
 - 「情報資産の洗い出し」の手順を詳細化し、その前に存在していた「リスク及び機会の特定」の手順を削除。
 - 機密性レベルのデフォルトを「公開・社外秘・極秘」に変更。また、『情報セキュリティ管理策規程』内に統合した「5.12 情報の分類」では、定義せず、マニュアル内の定義を参照する形に変更。
 - 発生頻度レベルの定義を変更。
 - 資産価値は影響度に置き換えず、そのままリスク値の算出式に利用する形に変更。
 - 資産価値の計算方法のデフォルトを「 $\{ \text{資産価値} \} = \{ \text{機密性の評価値} \} \times \{ \text{完全性の評価値} \} \times \{ \text{可用性の評価値} \}$ 」に変更。
 - 想定される脅威の特定、脆弱性の特定を追加。
 - 受容基準のデフォルトを「24」に変更。
- 「6.1.3 情報セキュリティリスク対応」
 - 『情報セキュリティリスクアセスメント手順』の内容を統合。
- 「7.2 力量」
 - 『情報セキュリティ教育・訓練手順』の内容を統合。
- 「7.5 文書化した情報」
 - 『標準類管理規程』の内容を統合。
- 「9.1 監視、測定、分析及び評価」
 - 監視・測定の記入欄を表形式に変更。
- 「9.2 内部監査」
 - 『内部監査規程』の内容を統合。
 - 「3年間の監査プログラムを『監査プログラム』に策定する」としていたが、「3年間で一回監査すればいい」という誤解を招くため、帳票『監査プログラム』を削除。
 - 指摘区分の定義を追加。
- 「9.3 マネジメントレビュー」
 - 『マネジメントレビュー規程』の内容を統合。
 - マネジメントレビューのインプットに関する記述を追加。
 - デフォルトの承認手順を修正。
- 「10.2 不適合及び是正処置」
 - 『是正・予防処置規程』の内容を統合。



【変更点】

- JIS Q 27001:2023 (ISO/IEC 27001:2022) の附属書 A に記載されている管理策に関連する管理規程について、『情報セキュリティ管理策規程』に統合。
- 『情報セキュリティ管理策規程』内の管理策の順序は、JIS Q 27001:2023 (ISO/IEC 27001:2022) の附属書 A の管理策の順序にあわせて変更。
- 「5.12 情報の分類」
 - 機密性レベルの定義は、『情報セキュリティマニュアル』内「6.1.2 情報セキュリティリスクアセスメント」の定義を参照する形に変更。

組織の状況を記載する帳票の追加



【変更点】

- 『組織状況管理表』を追加。
- 『情報セキュリティマニュアル』に記載されていた、外部の課題、内部の課題、利害関係者 及び利害関係者の要求事項 を『組織状況管理表』に記載する形に変更。

情報セキュリティリスクアセスメント・リスク対応にかかる帳票の統合・名称変更

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『情報資産管理台帳』 <input type="checkbox"/> 『情報セキュリティリスクアセスメント表』		<input type="checkbox"/> 『情報資産リスクアセスメント表』

【変更点】

- Excel マクロ有効ファイル『情報資産関連帳票作成シート』の廃止
- 『情報資産管理台帳』と『情報セキュリティリスクアセスメント表』を『情報資産リスクアセスメント表』に統合。
- リスクアセスメント手順の変更に伴い、資産価値の算出方法を CIA の和 から CIA の積 に変更。
- 残留リスクがあった場合のリスク所有者による承認欄を追加。

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『情報セキュリティリスク対応計画』		<input type="checkbox"/> 『情報セキュリティリスク対応計画表』

【変更点】

- 名称を『情報セキュリティリスク対応計画表』に変更。
- 入力項目を整理。
- リスク所有者が複数の人に分かれている場合を想定し、各リスク対応計画について承認した記録を記載する欄を追加。
- 計画スケジュール及び実施結果を記載する欄を追加。
- リスク対応計画の実施結果について評価を記録する欄を追加。

適用宣言書の改善

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『適用宣言書』		<input type="checkbox"/> 『適用宣言書』

【変更点】

- ファイル形式を、Word ファイル から Excel ファイルに変更。
- 管理策の採否理由と実施状況の記載欄を分離。

組織の要員の力量を記載する帳票の名称変更

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『有資格者リスト』		<input type="checkbox"/> 『スキル管理表』

【変更点】

- いわゆる資格だけでなく、組織が定義した力量を満たしている要員を管理する帳票だった『有資格者リスト』は、名称からその役割を読み取れなかったため、『スキル管理表』に名称を変更。

文書管理台帳の統合

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『標準類管理台帳』		<input type="checkbox"/> 『文書管理台帳』
<input type="checkbox"/> 『外部文書管理台帳』		

【変更点】

- 『標準類管理台帳』と『外部文書管理台帳』を統合し、『文書管理台帳』に名称を変更。
- 『文書管理台帳』で、内部文書も外部文書も扱えるように、項目を変更。

監査プログラムの削除

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『監査プログラム』		なし

【変更点】

- 主要でないものについては3年間でサンプリングを想定していたが、初回は全てに対して監査を実施する必要があるため、文書サンプルで「3年間でサンプリング可能であること」を示唆しないように、『監査プログラム』を削除。

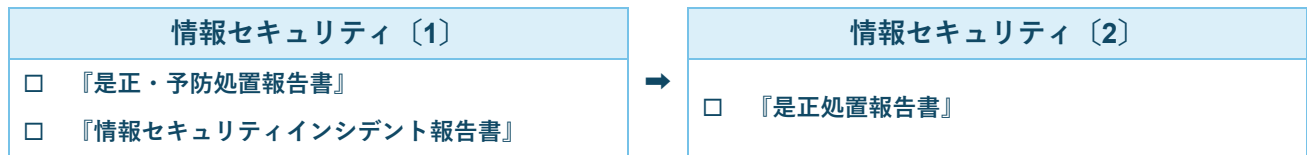
パフォーマンス評価表の削除

情報セキュリティ〔1〕	→	情報セキュリティ〔2〕
<input type="checkbox"/> 『パフォーマンス評価表』		なし

【変更点】

- パフォーマンス評価は、別の帳票を監視・測定結果の証拠とするものとし、当該帳票は削除。

是正処置報告書の改善



【変更点】

- 名称を『是正処置報告書』に変更。
- 『情報セキュリティインシデント報告書』を統合。
- 「該当規格」を「対象となるルール」に変更し、不適合事象が適合していないルール・規程を記載できるように変更。
- 帳票の構成を変更し、大きく分けて「不適合」「修正処置」「是正・予防処置」「是正・予防処置のレビュー」から構成され、レビューの実施日・実施者・レビュー内容について記載する欄を追加。
- 「水平展開の必要性」について、「修正処置」のパートに移動。

その他変更点

- 文書サンプル内、[テキストコンテンツコントロールの（例）](#) 及び [青色の背景の部分](#) は、参考例となります。お客様の状況・決定に則した形に修正いただくことを強く推奨いたします。

今後の予定

アームスタンダードでは、お客様からのご意見・ご要望をもとに、随時文書サンプルの見直し・改善をおこなっております。

今回のリリースでは対応しきれない改善点についても、引き続き改修を進めてまいります。

今後は、今回のような形で少なくとも年に1度、文書体系サンプルの新しいバージョンをご案内していく予定です。

アームスタンダード株式会社 IT トレーナー事務局

〒103-0012 東京都中央区日本橋堀留町 1-10-15 JL 日本橋ビル 1F

E-mail : trainer@armstandard.com

TEL : 03-3666-8788

FAX : 03-3666-8752

URL : <https://www.armstandard.com>