Sec02-01CyberSec Diary

[Sec02-01CyberSec Diary 1](#_Toc499883890)

[1. 中小企業サイバーセキュリティ対策関連の備忘録 15](#_Toc499883891)

[1.1. 緊急対応時のピックアップ情報 15](#_Toc499883892)

[1.2. 情報セキュリティが心配になったら - CyberSec diary 15](#_Toc499883893)

[1.3. 相談対応手引き関連 15](#_Toc499883894)

[1.3.1. •サイバーセキュリティ相談・届出先クイックリスト - CyberSec diary 15](#_Toc499883895)

[1.3.2. •情報セキュリティ緊急対応ガイド【汎用】 - CyberSec diary 15](#_Toc499883896)

[1.3.3. •相談対応の手引きレファレンスリスト【相談員用】 - CyberSec diary 15](#_Toc499883897)

[1.3.4. •サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec diary 15](#_Toc499883898)

[1.4. 事例（FAQ候補） 15](#_Toc499883899)

[1.4.1. •セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary 15](#_Toc499883900)

[1.4.2. •ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec diary 15](#_Toc499883901)

[1.5. 情報化推進のためのセキュリティ対策 15](#_Toc499883902)

[1.5.1. デジタルトランスフォーメーション時代のセキュリティ対策 15](#_Toc499883903)

[1.6. 中小企業向けの情報セキュリティ対策関連 15](#_Toc499883904)

[1.6.1. 中小企業の情報セキュリティ対策ガイドライン 15](#_Toc499883905)

[1.6.2. •中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 【パブリックコメント中】 38](#_Toc499883906)

[1.6.3. サイバーセキュリティ経営ガイドライン 39](#_Toc499883907)

[1.6.4. 企業経営のためのサイバーセキュリティの考え方 39](#_Toc499883908)

[1.6.5. その他 39](#_Toc499883909)

[1.7. 家庭個人向け 39](#_Toc499883910)

[1.7.1. •家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec diary【更新中】 39](#_Toc499883911)

[1.8. 重要インフラ関連 39](#_Toc499883912)

[1.8.1. •重要インフラ・大企業向けサイバーセキュリティ対策 - CyberSec diary【更新中】 39](#_Toc499883913)

[1.9. 政府機関等向け 39](#_Toc499883914)

[1.9.1. 政府機関向けサイバーセキュリティ対策 - CyberSec diary【更新中】 39](#_Toc499883915)

[1.10. 情報セキュリティマネジメント関連 40](#_Toc499883916)

[1.10.1. •サイバーセキュリティとは - CyberSec diary 40](#_Toc499883917)

[1.10.2. •情報セキュリティに関する基礎知識 - CyberSec diary 40](#_Toc499883918)

[1.10.3. •情報セキュリティ対策の概念 - CyberSec diary 40](#_Toc499883919)

[1.10.4. •情報セキュリティポリシー、実施手順 - CyberSec diary 40](#_Toc499883920)

[1.10.5. •情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary 40](#_Toc499883921)

[1.10.6. •セキュリティインシデント対応は事業継続計画（BCP）の一つ - CyberSec diary 40](#_Toc499883922)

[1.11. 人材育成・人材確保 40](#_Toc499883923)

[1.11.1. •小規模サイトにおける情報システム担当者が持つべき知識とスキル - CyberSec diary 40](#_Toc499883924)

[1.11.2. •情報セキュリティマネジメントに必要な知識 - CyberSec diary 40](#_Toc499883925)

[1.12. 関連基準、法規、対策機関等 40](#_Toc499883926)

[1.12.1. •サイバーセキュリティに関連したガイドライン等インデックス - CyberSec diary 40](#_Toc499883927)

[1.12.2. •政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec diary 40](#_Toc499883928)

[1.12.3. •情報セキュリティ関連法規リスト（更新中） - CyberSec diary 40](#_Toc499883929)

[1.12.4. •サイバーセキュリティ対策公的機関・関連団体・関連機関インデックス - CyberSec diary 40](#_Toc499883930)

[1.13. セキュリティ関連情報提供サイト一覧 40](#_Toc499883931)

[1.13.1. •サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポータルサイト - CyberSec diary 40](#_Toc499883932)

[1.14. ニュース 40](#_Toc499883933)

[1.14.1. •中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 【パブリックコメント中】 40](#_Toc499883934)

[1.14.2. •「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec diary 40](#_Toc499883935)

[2. 緊急対応時のピックアップ情報 40](#_Toc499883936)

[3. 情報セキュリティが心配になったら - CyberSec diary 40](#_Toc499883937)

[3.1. 【緊急】どんな環境で何が起きてますか？まずは落ち着いて今起きている事象を確認しましょう 41](#_Toc499883938)

[3.1.1. •セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式) 41](#_Toc499883939)

[3.2. 【緊急】セキュリティ侵害の可能性があるが、どこに問い合せていいかわからない? 41](#_Toc499883940)

[3.2.1. •「中小企業サイバーセキュリティ対策相談窓口」へ 41](#_Toc499883941)

[3.3. 【緊急】情報の漏えい・改ざんが起きている？ 41](#_Toc499883942)

[3.3.1. •犯罪の可能性がある場合は、警視庁へ 41](#_Toc499883943)

[3.4. 【緊急】PC、スマホの動きがおかしくなった、データが壊れた? 41](#_Toc499883944)

[3.4.1. •ウイルス感染、不正アクセスの可能性 41](#_Toc499883945)

[3.5. 【緊急】実被害にあった場合 41](#_Toc499883946)

[3.5.1. •同様の被害を拡大させないためにも、速やかに届けてください。 41](#_Toc499883947)

[3.5.2. •ウイルス・不正アクセス届出 41](#_Toc499883948)

[3.5.3. •インシデント報告・届出 41](#_Toc499883949)

[3.5.4. •サイバー犯罪届出（全国） 41](#_Toc499883950)

[3.6. 【相談】セキュリティ関連の各種相談、問合せ 42](#_Toc499883951)

[3.6.1. •嫌がらせ、ネットストーカーの相談 42](#_Toc499883952)

[3.6.2. •ECサイトのなりすまし被害 42](#_Toc499883953)

[3.7. 【一般】セキュリティに限らず、消費生活全般に関する苦情や問合せ先は？ 42](#_Toc499883954)

[3.7.1. •消費者ホットライン 42](#_Toc499883955)

[3.7.2. •暮らしにかかわる東京都の情報サイト 42](#_Toc499883956)

[3.8. 【事前予防】情報セキュリティ侵害に遭わないように事前に対処しておきましょう 42](#_Toc499883957)

[3.8.1. •情報セキュリティ対策の基本を知る 42](#_Toc499883958)

[3.9. 【知識】情報セキュリティ対策の必要性を認識し、網羅的な対策を知るには？ 42](#_Toc499883959)

[3.9.1. •中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 42](#_Toc499883960)

[3.9.2. •教育・学習（企業・組織向け）｜ここからセキュリティ！ 情報セキュリティ・ポータルサイト 43](#_Toc499883961)

[3.9.3. •企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】(pdf形式) 43](#_Toc499883962)

[3.10. 参考情報 43](#_Toc499883963)

[3.10.1. 信頼性の高いセキュリティ対策情報を提供しているサイトの内容を解説します 43](#_Toc499883964)

[3.10.2. 中小企業向けサイバーセキュリティ関連ニュース 43](#_Toc499883965)

[3.11. 他のページへのリンク 43](#_Toc499883966)

[3.11.1. 中小企業サイバーセキュリティ対策関連の備忘録 - CyberSec diary 43](#_Toc499883967)

[4. •サイバーセキュリティ相談・届出先クイックリスト - CyberSec diary 43](#_Toc499883968)

[4.1. 凍結中 43](#_Toc499883969)

[5. •情報セキュリティ緊急対応ガイド【汎用】 - CyberSec diary 43](#_Toc499883970)

[5.1. ■緊急対応（自然災害, 大火災, 感染症, テロ, , ,） 43](#_Toc499883971)

[5.1.1. 事象の検知、報告受付(Detect) 43](#_Toc499883972)

[5.1.2. 事実確認、対応の判断 被害の局所化(拡大防止)(Triage) 43](#_Toc499883973)

[5.1.3. 緊急連絡 44](#_Toc499883974)

[5.1.4. 原状保全 44](#_Toc499883975)

[5.1.5. 原因調査 44](#_Toc499883976)

[5.1.6. 早期復旧・事業継続 (Respond) 44](#_Toc499883977)

[5.1.7. 恒久的対策（再発防止策） 44](#_Toc499883978)

[5.1.8. 通常運用 44](#_Toc499883979)

[5.2. ■情報セキュリティ対策の必要性 44](#_Toc499883980)

[5.2.1. •ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、セキュリティ侵害、、）が発生して、事業資産（人・もの（情報及び設備）・金）、社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性がある。 44](#_Toc499883981)

[5.2.2. •どんな緊急事態が発生しても、事業を継続できるようにする対策を明示しておくことが必要 45](#_Toc499883982)

[5.2.3. •情報セキュリティ対策は、事業継続計画の一つ 45](#_Toc499883983)

[5.2.4. •サービスの向上を図るために、情報資産（保有情報（媒体に依らず）、情報機器、情報システム）に対する情報セキュリティ上のリスクを低減させる 45](#_Toc499883984)

[5.2.5. •ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用の中で実施すべき先行投資であり、緊急事態が発生した後に対処する経費として想定してはいけない 45](#_Toc499883985)

[5.3. ■情報セキュリティ対策の基本 45](#_Toc499883986)

[5.3.1. 情報セキュリティ侵害とは 45](#_Toc499883987)

[5.3.2. 脅威・手口を知る（10大脅威2016簡易説明資料（組織編）） 45](#_Toc499883988)

[5.3.3. 情報資産の認識 45](#_Toc499883989)

[5.3.4. リスク分析 45](#_Toc499883990)

[5.3.5. 対策はリスクの高いものを優先する 46](#_Toc499883991)

[5.3.6. 恒久的対策 46](#_Toc499883992)

[5.3.7. 定期的な監査 47](#_Toc499883993)

[5.4. ■参考資料 47](#_Toc499883994)

[6. •相談対応の手引きレファレンスリスト【相談員用】 - CyberSec diary 47](#_Toc499883995)

[6.1. ■信頼性の高いセキュリティ対策情報を提供しているサイトの内容の解説 47](#_Toc499883996)

[6.1.1. •ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec diary 47](#_Toc499883997)

[6.2. ■事例等の紹介 47](#_Toc499883998)

[6.2.1. •セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary 47](#_Toc499883999)

[6.3. ■対策まとめ資料 47](#_Toc499884000)

[6.3.1. •情報セキュリティ対策とは 47](#_Toc499884001)

[6.3.2. •中小企業向け対策 47](#_Toc499884002)

[6.3.3. •システム調達におけるセキュリティ要件定義 47](#_Toc499884003)

[6.3.4. ――――――――相談対応の手引き用【更新中】―――――― 47](#_Toc499884004)

[7. •サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec diary 48](#_Toc499884005)

[7.1. •サイバーセキュリティ対策相談対応の手引き（メモ） 48](#_Toc499884006)

[7.1.1. 展開した文書 48](#_Toc499884007)

[8. •セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary 48](#_Toc499884008)

[8.1. 各種Webから抜粋したページ 48](#_Toc499884009)

[8.2. ◦相談窓口対応事例（FAQ候補） - CyberSec diary 48](#_Toc499884010)

[9. •ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec diary 48](#_Toc499884011)

[9.1. 「ここからセキュリティ」を展開したページ 48](#_Toc499884012)

[10. •IT化・デジタル化により業務の効率化・サービスの向上を図るために、セキュリティ対策を実施【私見】 48](#_Toc499884013)

[10.1. ■デジタルトランスフォーメーション時代の情報セキュリティ対策 48](#_Toc499884014)

[10.1.1. ●IT活用の必然性と情報セキュリティ対策の必要性 48](#_Toc499884015)

[10.1.2. セキュリティ侵害の実態 50](#_Toc499884016)

[10.1.3. 情報セキュリティ対策の必要性の認識が必要 50](#_Toc499884017)

[10.1.4. システムをベンダーに任せて開発もしくは導入、運用している 51](#_Toc499884018)

[10.1.5. 効果的な情報セキュリティ対策の方法がわからない 51](#_Toc499884019)

[11. •デジタルトランスフォーメーション時代のITとデジタル情報の活用 - CyberSec diary　【作成中】 51](#_Toc499884020)

[11.1. 【作成中】 52](#_Toc499884021)

[11.2. ■活用戦略 52](#_Toc499884022)

[11.3. ■活用技術 52](#_Toc499884023)

[11.4. ●クラウドコンピューティング 52](#_Toc499884024)

[12. 中小企業に特化した情報セキュリティ対策の相談対応【私見】 - CyberSec diary 52](#_Toc499884025)

[12.1. 対象範囲と役割分担 52](#_Toc499884026)

[12.2. 中小企業の現状 52](#_Toc499884027)

[12.2.1. •組織の意識と対策 52](#_Toc499884028)

[12.2.2. •実態調査 52](#_Toc499884029)

[12.3. 中小企業への支援 52](#_Toc499884030)

[12.3.1. •普及啓発 53](#_Toc499884031)

[12.3.2. •対策の概要 53](#_Toc499884032)

[13. •中小企業経営者向けセキュリティ対策情報のレファレンスリスト - CyberSec diary 54](#_Toc499884033)

[13.1. ■緊急相談対応 54](#_Toc499884034)

[13.1.1. •サイバーセキュリティ相談・届出先クイックリスト - CyberSec diary 54](#_Toc499884035)

[13.1.2. •セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式) 54](#_Toc499884036)

[13.1.3. •情報セキュリティに関する基礎知識 - CyberSec diary 54](#_Toc499884037)

[13.1.4. •情報セキュリティ緊急対応ガイド– CyberSec diary 55](#_Toc499884038)

[13.2. ■中小企業経営者向け情報 55](#_Toc499884039)

[13.2.1. •情報セキュリティ対策９カ条【NISC,IPA】(pdf形式) 55](#_Toc499884040)

[13.2.2. •5分でできる！情報セキュリティポイント学習【オンライン】【ダウンロード】【IPA】 55](#_Toc499884041)

[13.2.3. •企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】(pdf形式) 55](#_Toc499884042)

[13.2.4. •中小企業のためのセキュリティツールライブラリ一覧【IPA】 55](#_Toc499884043)

[13.2.5. •その他の各種情報へのリンク 55](#_Toc499884044)

[13.3. ■家庭・個人向け情報 56](#_Toc499884045)

[13.3.1. •【準備中】 56](#_Toc499884046)

[13.4. ■サイバーセキュリティ対策公的機関・関連団体・関連機関 56](#_Toc499884047)

[13.4.1. •サイバーセキュリティ対策公的機関・関連団体・関連機関インデックス - CyberSec diary（準備中） 56](#_Toc499884048)

[13.5. ■体系的・網羅的な情報を提供しているポータルサイト 56](#_Toc499884049)

[13.5.1. •サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポータルサイト - CyberSec diary 56](#_Toc499884050)

[13.6. ■人材育成・人材確保 56](#_Toc499884051)

[13.6.1. •小規模サイトにおける情報システム担当者が持つべき知識とスキル - CyberSec diary 56](#_Toc499884052)

[13.6.2. •情報セキュリティマネジメント -- XMind Online Library 56](#_Toc499884053)

[13.7. ■参考情報 56](#_Toc499884054)

[13.7.1. •サイバーセキュリティに関連したガイドライン等インデックス - CyberSec diary 56](#_Toc499884055)

[13.7.2. •情報セキュリティ関連法規リスト（更新中） - CyberSec diary 56](#_Toc499884056)

[13.7.3. •政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec diary 56](#_Toc499884057)

[13.8. ■関連ニュース 56](#_Toc499884058)

[13.9. ―――――― 相談対応の手引き用 ――――― 56](#_Toc499884059)

[13.9.1. ■信頼性の高いセキュリティ対策情報を提供しているサイトの内容の解説 56](#_Toc499884060)

[13.9.2. ■事例等の紹介 56](#_Toc499884061)

[13.9.3. ■対策まとめ資料 56](#_Toc499884062)

[13.10. ――――――――相談対応の手引き用【更新中】―――――― 57](#_Toc499884063)

[13.10.1. 【更新中】 57](#_Toc499884064)

[14. •中小企業に特化した情報セキュリティ対策の相談対応 - CyberSec diary 57](#_Toc499884065)

[14.1. ■対象範囲と役割分担 57](#_Toc499884066)

[14.2. ■中小企業の現状 57](#_Toc499884067)

[14.3. ■中小企業への支援 57](#_Toc499884068)

[15. •中小企業のサイバーセキュリティ対策インデックス（経営者・管理者・従業員） - CyberSec diary 57](#_Toc499884069)

[15.1. ■サイバーセキュリティ対策の必要性 57](#_Toc499884070)

[15.1.1. •情報セキュリティの脅威 57](#_Toc499884071)

[15.1.2. •守るべき情報資産の認識 57](#_Toc499884072)

[15.1.3. •最低限の対策 57](#_Toc499884073)

[15.2. ■理解度確認 57](#_Toc499884074)

[15.3. ■対策のしおり 57](#_Toc499884075)

[15.4. ■中小企業のサイバーセキュリティ対策にフォーカスした体系的・網羅的な情報 57](#_Toc499884076)

[15.4.1. ※主なサイトへのリンク 57](#_Toc499884077)

[15.5. ■個人のサイバーセキュリティ対策にフォーカスした体系的・網羅的な情報 57](#_Toc499884078)

[15.5.1. ※主なサイトへのリンク 57](#_Toc499884079)

[16. •家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec diary【更新中】 58](#_Toc499884080)

[16.1. 更新中 58](#_Toc499884081)

[17. •重要インフラ・大企業向けサイバーセキュリティ対策 - CyberSec diary【更新中】 58](#_Toc499884082)

[17.1. 重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ（案）【NISC】 58](#_Toc499884083)

[17.1.1. http://www.nisc.go.jp/conference/cs/dai07/pdf/07shiryou02.pdf 58](#_Toc499884084)

[17.2. サイバーセキュリティ経営ガイドライン【2016年12月METI】 58](#_Toc499884085)

[17.2.1. サイバーセキュリティ経営ガイドラインVer 1.1【2016年12月METI】 58](#_Toc499884086)

[17.2.2. サイバーセキュリティ経営ガイドライン Ver1.1（Ver1.0との差分）【2016年12月METI】（PDF形式） 58](#_Toc499884087)

[17.2.3. サイバーセキュリティ経営ガイドラインVer 1.1付録Ｂ－２ 技術対策の例【2016年12月METI】 58](#_Toc499884088)

[17.3. サイバーセキュリティ経営ガイドライン解説書【2016年12月IPA】 58](#_Toc499884089)

[17.3.1. 解説書：サイバーセキュリティ経営ガイドライン解説書（PDF：3.7MB） 58](#_Toc499884090)

[17.3.2. 別添　：被害事例集（Excel：78.9KB） 58](#_Toc499884091)

[18. 政府機関向けサイバーセキュリティ対策 - CyberSec diary【新規更新中】 58](#_Toc499884092)

[18.1. NISC第９回会合（持ち回り開催）（平成２８年８月３１日） 58](#_Toc499884093)

[18.1.1. http://www.nisc.go.jp/conference/cs/index.html 58](#_Toc499884094)

[18.1.2. サイバーセキュリティ2016 58](#_Toc499884095)

[18.1.3. 政府機関の情報セキュリティ対策のための統一規範 59](#_Toc499884096)

[18.1.4. 政府機関等の情報セキュリティ対策の運用等に関する指針 59](#_Toc499884097)

[18.1.5. 政府機関の情報セキュリティ対策のための統一基準（平成28年度版） 59](#_Toc499884098)

[18.1.6. サイバーセキュリティ政策の評価に係る基本方針 59](#_Toc499884099)

[19. •サイバーセキュリティとは - CyberSec diary 59](#_Toc499884100)

[19.1. ■サイバーセキュリティとは 59](#_Toc499884101)

[19.1.1. •サイバーとは 59](#_Toc499884102)

[19.1.2. •サイバー攻撃とは、 59](#_Toc499884103)

[19.1.3. •サイバーセキュリティとは 59](#_Toc499884104)

[19.1.4. •サイバーセキュリティ基本法において、 59](#_Toc499884105)

[20. •情報セキュリティに関する基礎知識 - CyberSec diary 59](#_Toc499884106)

[20.1. 1.1. 情報セキュリティ対策の基本 60](#_Toc499884107)

[20.2. 1.2. 【対策】情報セキュリティ 10 大脅威（個人） 60](#_Toc499884108)

[20.3. 1.3. 【対策】情報セキュリティ 10 大脅威（組織） 60](#_Toc499884109)

[20.4. 1.4. 【対策】注目すべき脅威や懸念 60](#_Toc499884110)

[20.5. 1.5 サービス提供と情報セキュリティ対策 60](#_Toc499884111)

[21. •情報セキュリティ対策の概念 - CyberSec diary 60](#_Toc499884112)

[21.1. 1.1. リスクの要因 60](#_Toc499884113)

[21.2. 1.2. 情報セキュリティにおけるさまざまな対策 60](#_Toc499884114)

[21.3. 1.3. 情報セキュリティ対策の意義 60](#_Toc499884115)

[21.4. 1.4. 情報セキュリティ対策のポイント（私見） 60](#_Toc499884116)

[22. •情報セキュリティポリシー、実施手順 - CyberSec diary 60](#_Toc499884117)

[22.1. 1.1. 情報セキュリティポリシーの構成 60](#_Toc499884118)

[22.2. 1.2. 情報セキュリティポリシー（基本方針） 60](#_Toc499884119)

[22.3. 1.3. 情報セキュリティポリシー（対策基準） 60](#_Toc499884120)

[22.4. 1.4. 情報セキュリティ実施手順 60](#_Toc499884121)

[22.5. 1.5. 情報セキュリティマネジメントシステム（ISMS）構築手順 60](#_Toc499884122)

[22.6. 1.6. ISMSとPDCAサイクル 60](#_Toc499884123)

[22.7. 1.7. 脅威・対策・脆弱性・リスクの関係 60](#_Toc499884124)

[22.8. 1.8. 情報セキュリティマネジメントの規格や標準 60](#_Toc499884125)

[22.8.1. 1.8.1. 情報セキュリティマネジメントの実践のための規範JIS Q 27002:2006 60](#_Toc499884126)

[22.8.2. 1.8.2. 情報セキュリティマネジメントシステム - 要求事項JIS Q 27001:2006 60](#_Toc499884127)

[22.9. 1.9. リスクマネジメント 60](#_Toc499884128)

[22.9.1. 1.9.1. 情報資産の格付け 60](#_Toc499884129)

[22.9.2. 1.9.2. ITセキュリティマネジメントのための手法（JIS TR X 0036-3:2001） 60](#_Toc499884130)

[23. •情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary 60](#_Toc499884131)

[23.1. 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」 60](#_Toc499884132)

[23.2. 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」に示された要件のうち、特にセキュリティに関連する部分を抜粋し、解説を加えたもの。 60](#_Toc499884133)

[23.3. 1.1. プロジェクトの管理 61](#_Toc499884134)

[23.4. 1.2. 業務の見直し 61](#_Toc499884135)

[23.5. 1.3. 要件定義 61](#_Toc499884136)

[23.6. 1.4. 設計・開発 61](#_Toc499884137)

[23.7. 1.5. 業務の運営と改善 61](#_Toc499884138)

[23.8. 1.6. 運用及び保守 61](#_Toc499884139)

[23.9. 1.7. システム監査の計画 61](#_Toc499884140)

[24. •セキュリティインシデント対応は事業継続計画（BCP）の一つ - CyberSec diary 61](#_Toc499884141)

[24.1. ■BCPとは 61](#_Toc499884142)

[24.2. ■BCPはなぜ必要か？ 61](#_Toc499884143)

[24.3. ■何のためにBCPを策定するのか？ 61](#_Toc499884144)

[24.4. ■セキュリティインシデント対応はBCPの１つ 61](#_Toc499884145)

[25. •小規模サイトにおける情報システム担当者が持つべき知識とスキル - CyberSec diary 61](#_Toc499884146)

[25.1. 1.1. ITパスポート試験シラバス 61](#_Toc499884147)

[25.2. 1.2. まとめ）企業の情報セキュリティ対策と人材面の対策 61](#_Toc499884148)

[25.3. 1.3. 情報処理技術者試験　情報セキュリティ人材育成の取り組み 61](#_Toc499884149)

[25.4. 1.4. 情報セキュリティマネジメント試験　シラバス 61](#_Toc499884150)

[25.5. 1.5. 情報セキュリティマネジメントタスクプロフィール 61](#_Toc499884151)

[25.6. 1.6. 情報セキュリティ人材の職種 61](#_Toc499884152)

[26. •情報セキュリティマネジメントに必要な知識 - CyberSec diary 61](#_Toc499884153)

[27. •サイバーセキュリティに関連したガイドライン等インデックス - CyberSec diary 61](#_Toc499884154)

[27.1. ◦公的機関、教育機関向け、個人ユーザー向け、事業者向け 61](#_Toc499884155)

[27.2. 「ここからセキュリティ！情報セキュリティ・ポータルサイト」>「対策する」>「ガイドライン等」より抜粋し補足説明。 61](#_Toc499884156)

[27.3. • 公的機関 61](#_Toc499884157)

[27.4. •教育機関向け 61](#_Toc499884158)

[27.5. •個人ユーザー向け 61](#_Toc499884159)

[27.6. •事業者向け 61](#_Toc499884160)

[28. •政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec diary 62](#_Toc499884161)

[28.1. ※全体的内容、規定の趣旨、対策例 62](#_Toc499884162)

[29. •情報セキュリティ関連法規リスト（更新中） - CyberSec diary 62](#_Toc499884163)

[29.1. 1.1. サイバーセキュリティ基本法 62](#_Toc499884164)

[29.2. 1.2. 不正アクセス禁止法 62](#_Toc499884165)

[29.3. 1.3. 個人情報保護法 62](#_Toc499884166)

[29.4. 1.4. 刑法 62](#_Toc499884167)

[29.5. 1.5. その他のセキュリティ関連法規 62](#_Toc499884168)

[29.6. 1.6. 知的財産権 62](#_Toc499884169)

[29.7. 1.7. 労働関連・取引関連法規 62](#_Toc499884170)

[29.8. 1.8. その他の法律・ガイドライン・技術者倫理 62](#_Toc499884171)

[30. •サイバーセキュリティ対策公的機関・関連団体・関連機関インデックス - CyberSec diary 62](#_Toc499884172)

[30.1. •関連サイト [内閣サイバーセキュリティセンター] 62](#_Toc499884173)

[30.2. •関連リンク：IPA 独立行政法人 情報処理推進機構 62](#_Toc499884174)

[30.3. •不正アクセス防止対策に関する官民意見集約委員会（官民ボード） 62](#_Toc499884175)

[30.4. •サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ）） 62](#_Toc499884176)

[30.5. •東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss: Tokyo Cyber Security Support network for small and medium enterprises） 62](#_Toc499884177)

[31. •サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポータルサイト - CyberSec diary 62](#_Toc499884178)

[31.1. •情報セキュリティって何をするの？「ここからセキュリティ！」:情報セキュリティ・ポータルサイト（事象・対象別） 【管理者：情報処理推進機構(IPA)】 62](#_Toc499884179)

[31.1.1. ◦「不正アクセス防止対策に関する官民意見集約委員会(官民ボード)に参加している内閣官房、警察庁、総務省及び経済産業省と民間事業者等が提供している信頼性が高く網羅的な情報群を事象・対象別に分類してナビゲートするポータルサイトです。 62](#_Toc499884180)

[31.2. •サイトマップ[みんなでしっかりサイバーセキュリティ]【内閣官房サイバーセキュリティセンター(NISC)】 62](#_Toc499884181)

[31.2.1. ◦NISCが運営するサイバーセキュリティに関する情報のポータルです。 「スマートフォン利用者の方へ」、「家庭で」、「学校で」、「会社で」、「困ったときに」というカテゴリ別に、簡単かつ網羅的に解説されてます。 63](#_Toc499884182)

[31.3. •国民のための情報セキュリティサイト【総務省】 63](#_Toc499884183)

[31.3.1. ◦インターネットと情報セキュリティの知識の習得に役だち、利用方法に応じた情報セキュリティ対策を講ずるための基本となる情報を提供しています。 63](#_Toc499884184)

[31.4. •情報セキュリティ広場【警視庁】 63](#_Toc499884185)

[31.4.1. ◦安全な暮らしのための情報の一環で、情報セキュリティに関連する情報を体系的にわかりやすく提供しています。サイバー犯罪相談と検挙事例を通してサイバー犯罪から身を守るために必要な情報を広く都民の皆さんに提供することを目的としています。 インターネット関連企業等で構築されている「サイバー犯罪対策協議会」と連携をとって少しでもみなさんのお役に立てるページを作りました。 63](#_Toc499884186)

[31.5. •IS702【トレンドマイクロ】 63](#_Toc499884187)

[31.6. •Security & Trust : 企業ネットワークセキュリティのためのノウハウ＆情報フォーラム 【@IT】 63](#_Toc499884188)

[32. •中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 【パブリックコメント中】 63](#_Toc499884189)

[33. •「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec diary 63](#_Toc499884190)

[34. 国としての施策・基本方針・ガイドライン等の体系 63](#_Toc499884191)

[34.1. ISMS認証基準 63](#_Toc499884192)

[34.1.1. JIS Q 27000：2014 63](#_Toc499884193)

[34.1.2. JIS Q 27001:2014 63](#_Toc499884194)

[34.1.3. JIS Q 27002：2014 63](#_Toc499884195)

[34.1.4. 【参考】 64](#_Toc499884196)

[34.2. 「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（平成28年度版）」（2016年8月31日サイバーセキュリティ戦略本部決定） 64](#_Toc499884197)

[34.2.1. http://www.nisc.go.jp/active/general/kijun28.html 64](#_Toc499884198)

[34.3. 企業経営のためのサイバーセキュリティの考え方の策定について【NISC】 64](#_Toc499884199)

[34.3.1. http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf 64](#_Toc499884200)

[34.3.2. サイバーセキュリティ戦略本部 64](#_Toc499884201)

[34.3.3. 経営層に期待される“認識”や経営戦略を企画する人材層に向けた実装のためのツールを示す 64](#_Toc499884202)

[34.3.4. 基本方針 64](#_Toc499884203)

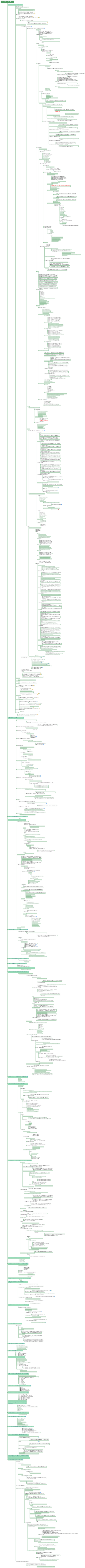
[34.3.5. I.基本的考え方 64](#_Toc499884204)

[34.3.6. II.企業の視点別の取組 65](#_Toc499884205)

[34.4. 「政府情報システムの整備及び管理に関する標準ガイドライン」(2015年3月19日更新、2014年12月3日各府省CIO連絡会議決定）および「実務手引書」 67](#_Toc499884206)

[34.4.1. http://www.soumu.go.jp/main\_sosiki/gyoukan/kanri/infosystem-guide.html 67](#_Toc499884207)

[34.4.2. 世界最先端IT国家創造宣言(2013年6月14日閣議決定。2014年6月24日変更)に基づき、政府におけるITガバナンス強化のため、情報システム調達やプロジェクト管理に関する共通ルールとして策定 67](#_Toc499884208)



# 中小企業サイバーセキュリティ対策関連の備忘録

## [緊急対応時のピックアップ情報](#____________________________________CyberSec_diary_2)

## [情報セキュリティが心配になったら - CyberSec diary](#____________________________________CyberSec_diary_2)

## 相談対応手引き関連

### [•サイバーセキュリティ相談・届出先クイックリスト - CyberSec diary](#____________________________CyberSec_diary_2)

### [•情報セキュリティ緊急対応ガイド【汎用】 - CyberSec diary](#________________________CyberSec_diary_2)

### [•相談対応の手引きレファレンスリスト【相談員用】 - CyberSec diary](#____________________________CyberSec_diary_4)

### [•サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec diary](#_____________________________CyberSec_diary_2)

## 事例（FAQ候補）

### [•セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary](#__________________FAQ______CyberSec_diary_2)

### [•ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec diary](#_______________________________IPA__FAQ______CyberSec_diary_2)

## 情報化推進のためのセキュリティ対策

### デジタルトランスフォーメーション時代のセキュリティ対策

#### [•IT化・デジタル化により業務の効率化・サービスの向上を図るために、セキュリティ対策を実施【私見】](#__IT_______________________________________________2)

#### [•デジタルトランスフォーメーション時代のITとデジタル情報の活用 - CyberSec diary　【作成中】](#_____________________IT_____________CyberSec_diary_______2)

## 中小企業向けの情報セキュリティ対策関連

### [中小企業の情報セキュリティ対策ガイドライン](http://www.ipa.go.jp/security/keihatsu/sme/guideline/)

#### [■中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】](http://www.ipa.go.jp/files/000055520.pdf)

##### 経営者の皆様へ

###### 情報セキュリティ対策は、経営に大きな影響を与えます！

###### 経営者が自ら動かなければ、法的・道義的責任を問われます！

###### 組織として対策するために、担当者への指示が必要です！

##### 対象組織と想定する読者

###### 経営者層・システム管理者層

###### 対象組織

本ガイドラインは、業種を問わず中小企業及び小規模事業者（法人のほか、個人事業  
主や各種団体も含む） 1を対象として作成されています。

###### 想定読者

組織の経営者と、経営者の指示のもとで重要な情報を管理する方を読者と想定して  
います。

##### 全体解説

###### （1）本ガイドラインの構成

本編２部と付録より構成

###### （2）本ガイドラインの使い方

①経営者の方

②経営者の指示のもとで重要な情報を管理する方

【図3】情報セキュリティ対策の進め方

Step1 まず始める

情報セキュリティ5か条

Step2 現状を知り改善する

情報セキュリティ自社診断

Step3 本格的に取り組む

情報セキュリティポリシーの策定

Step4 改善を続ける

情報セキュリティ対策のさらなる改善に向けて

##### 第 1部 経営者編

###### 情報セキュリティ対策を怠ることで企業が被る不利益

(1) 金銭の喪失

【表2】最近のサイバー攻撃等による情報漏えい等の経済的損失例

情報漏えい

教育サービス事業者で顧客の個人情報が3504件が漏えい（2014年）

システム開発・運用を行っている委託先の再委託先社員による不正取得と名簿の売却

株式を公開している雑貨卸事業者でインターネット上の株主向けサービスに登録された株主の個人情報6187件（他社の株主個人情報含め12014件）が漏えいした（2015年）

運営委託先サービスサイトへの不正アクセス

航空会社の顧客の個人情報4131件が漏えいした（2014年）

菓子食品製造事業者で個人情報29999件が漏えいした（2015年）

国内半導体製造事業者の技術jに関する機密情報が韓国の同業者に漏えい（2014年）

メガネ販売事業者でオンラインショップ顧客のクレジットカード情報2059件の漏えい（2013年）

ウイルス感染

米国の病院で院内ネットワークで共有する電子カルテシステムがウイルスによる攻撃により動作しなくなり診療不能に（2016年）

ランサムウェアに感染し、ファイルが暗号化されたため

ウェブサイト改ざん

観光バス事業者のホームページが改ざんされ閲覧するとウイルスに感染する恐れ（2014年）

(2) 顧客の喪失

(3) 業務 の喪失

(4) 従業員 への影響

###### 経営者が負う責任

(1) 経営者などに問われる法的責任

・個人情報

・他社から預かった秘密情報

・自社の秘密情報

・株価に影響を与える可能性のある未公開内部情報

(2) 関係者や社会に対する責任

・営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらずだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウン

法令順守・顧客・取引先・従業員

###### 経営者は何をすればよいか

[サイバーセキュリティ経営ガイドライン【2015年12月MEIT・IPA】の内容を中小企業向けに編集](http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf)

経営者が認識する必要な「３原則」

原則１ 情報セキュリティ対策は経営者のリーダシップのもとで進める

さまざまな脅威がもたらすリスクに対する対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策を実施します。

セキュリティ対策をしないことによる損失、対策に要する投資、ITの利活用を推進することによる利益を勘案して判断

セキュリティ対策をしないことによる損失＞対策に要する投資

ITの利活用を推進することによる利益＞対策に要する投資

原則２ 委託先における情報セキュリティ対策まで考慮する

自社同様に十分な注意を払い、必要に応じて委託先が実施している情報セキュリティ対策も確認

原則３ 情報セキュリティに関する関係者とのコミュニケーションは、どんなときにも怠らない

普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。

企業 として重要 として実施する「重要 7項目の取組」

取組１ 情報 セキュリティ に関するリスクを認識し組織全体での対応方針を定める

「当社は中小企業の情報セキュリティ対策ガイドラインに基づき情報セキュリティ対策を実践する。」「当社は顧客情報の流出防止を徹底することから情報セキュリティ対策を開始する。」

取組２ 情報セキュリティ対策を行うための資源（予約、人材など）を確保する

万が一事故（インシデント7）が起きてしまった場合、被害を最小限に止めるために、あらかじめ準備することも含みます。

取組３ 情報セキュリティのリスクを把握し、どこまで情報セキュリティ対策を行うのかを定めたうえで担当者に実行させる

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。検討した対策ごとに予算を与え、担当者を任命し、実行を指示します。

取組４ 情報セキュリティ対策に関する定期的な見直しを行う

最初から最適な形で実現することはどんな会社でも難しいもの。また情報技術は進化が早く、加えて脅威も変化します。

取組５ 業務委託する場合や外部ITシステムやサービスを利用する場合は、自社で必要と考える情報セキュリティ対策が担保されるようにする

契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する

利用規約やサービスに付随する情報セキュリティ対策等を確認したうえで選定するよう担当者に指示する

取組６ 情報セキュリティに関する最新動向を収集する

情報セキュリティに関する最新動向を発信している公的機関8などを把握しておき、常時参照することで、新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

取組７ 緊急時の社内外の連絡先や被害発生時に行うべき内容について準備しておく

万が一のインシデントに備えて、緊急時の連絡体制を整備します。、経営者の対応についても、あらかじめ決めておけば、冷静で的確な対応が可能になります。

##### 第 2部 管理実践編

###### 情報セキュリティ管理の進め方

【図5】ガイドラインの使用方法

###### 情報セキュリティ５か条

【表4】情報セキュリティ5か条

OSやソフトウェアは常に最新の状態にしよう！

ウイルス対策ソフトを導入しよう！

パスワードを強化しよう！

共有設定を見直そう！

脅威や攻撃の手口を知ろう！

###### 5分でできる！情報セキュリティ自社診断

Part1 基本的対策

Part2 従業員としての対策

Part3 組織としての対策

###### 情報セキュリティポリシーの策定

（1）基本的な考え方

① 自社に適合したポリシーを策定

【図6】セキュリティポリシー文書構成

② 情報セキュリティリスクの大きなものから重点的に対策を実施

【図7】リスクの「保有」の考え方

（2） ポリシー策定までの流れ

【図8】情報セキュリティポリシー策定までの流れ

手順１ 情報資産台帳を作成する

どのような情報資産があるか洗い出して重要度を判断する

●機密性、完全性、可用性それぞれの評価値11を記入します（表6）。

●機密性・完全性・可用性の評価値から重要度を判定します（表7）。

【表6】情報資産の機密性・完全性・可用性の評価基準

機密性・完全性・可用性→重要度

【表7】情報資産の重要度判断基準

付録の利用方法（手順１）

手順2 リスク値の算定

リスク値=重要度（機密性×完全性×機密性）×被害発生可能性の合計（脅威の起きる可能性×脆弱性の大きさ）

【表9】リスク値の算定基準

【表10】脅威例に応じたリスクのレベル

付録の利用方法（手順2）

手順3 情報セキュリティ対策を決定（対策を決める）

ア）リスクを低減する

　自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

イ）リスクを保有する

　事故が発生しても許容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

ウ）リスクを回避する

　仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

リスクを許容する

付録の利用方法（ツールA）

手順4 情報セキュリティポリシーを策定（対策をルールにする）

付録の利用方法（手順4）

【表11】情報セキュリティポリシーサンプル

1 組織的対策

2 人的対策

3 情報資産管理

4 マイナンバー対応

5 アクセス制御及び認証

6 物理的対策

7 IT機器利用

8 IT基盤運用管理

9 システムの開発及び保守

社内でシステム開発を行う場合

10 委託管理

業務委託を行う場合

11 情報セキュリティインシデント対応及び事業継続管理

12 社内体制図

従業員数２名以上

13 委託契約書サンプル

委託先と秘密情報や個人情報等の重要な情報の授受が発生する場合

（3）委託時の情報セキュリティ対策

（4）情報セキュリティ対策の実行

① 通常時の役割

経営者

管理者層

一般従業員

② 緊急時の対応

※しおり

① 緊急時の指揮命令と対応の優先順位の決定

② インシデントへの対応（インシデントレスポンス）

③ インシデントの影響と被害の分析

④ 情報収集と自社に必要な情報の選別

⑤ 社内関係者への連絡と周知

⑥ 外部関係機関との連絡

（5）チェックと改善

① チェックの方法

② 改善の方法

###### 情報セキュリティ対策のさらなる改善に向けて

（1）情報セキュリティマネジメントサイクルによる継続的改善

　ISO/IEC27001 が定めているマネジメントシステム（管理のしくみ）の考え方の基本は、Plan（計画）、Do（実行）、Check（チェック）、Act（改善）の４段階の活動（PDCA サイクル13）を順に繰り返すことを通じて改善していくことにあります。情報セキュリティ対策で見ると、それぞれ次の活動に相当します。

● Plan：情報セキュリティ対策の計画立案または見直し

● Do：情報セキュリティ対策の実践

● Check：監査・点検による活動の有効性確認と経営者による必要な改善箇所の決定

● Act：改善の実施

（2）情報セキュリティ対策に関する標準規格

付録３で示す対策は、中小企業でも取り組みやすいように情報セキュリティの国際規格であるISO/IEC 27002（情報セキュリティ管理策の実践のための規範）から抜粋し、解りやすい表現にしています。

（3）情報セキュリティ監査・点検の実施

● 質問（ヒアリング）：従業員や委託先の管理者などに直接質問して回答を求める

● 閲覧（レビュー）：情報セキュリティポリシーの関連手続きで申請書などの帳票や、コンピュータのログ、設定内容など実行の証拠となるものを見て確認する

● 観察（視察）：監査・点検者が現場に赴き、情報セキュリティ対策を行う当事者が情報セキュリティポリシーに従った行動をしていることを目視で確認する

● 技術診断：技術的対策の運用状況などについて、監査・点検者が自ら機器を操作することによって検証する（情報システムや社内ネットワークの脆弱性を確認するために、専用ソフトウェアを使い技術的な脆弱性を診断することもある）

（4）改善の実施

経営者や管理者層での議論、検討を通じて、情報セキュリティポリシーや具体的な対策に関する従業員や関係者の理解を促し、不備を改善し、今後に向けた改善につなげていきます。

##### おわりに

###### 

標的型攻撃の巧妙化により、適切な対策を実施していても被害を完全に防ぐこ  
とが困難になる中、異常事態の発生を素早く検知し、被害を最小限に抑制するための  
体制が注目されるなど、対策面も変化しています。また、マイナンバー法の施行、個人  
情報保護法の改正などに伴い、企業規模を問わず情報セキュリティに対する社会的要  
請、法的責任が拡大し、中小企業においても情報セキュリティへの取り組みは優先課  
題となっています。

　一方で、中小企業では依然として資金面や人材面での制約から情報セキュリティ対  
策の実施が難しいといわれており、実際の統計からも大企業に比較すれば対策が進ん  
でいない傾向が認められます。

。こうした状況を踏まえ、近年、変化・増大する脅威に対  
する情報セキュリティ対策を、適切かつ有効なものとすることを目的として、本ガイ  
ドラインの初版の内容を抜本的に見直し、改訂版を作成することとしました。

中小企業は情報セキュリティ対策に十分な経営資源を割り当てることができない  
という不利を抱える一方で、経営者を含め「従業員の顔が見える」という有利な条件を  
備えています。

情報セキュリティの第一歩は、経営者が情報セキュリティの重要性を  
自ら認識し、そのことを従業員に伝え、従業員がその対策を行う意義を理解すること  
です

。つまり、「従業員の顔が見える」ということは経営者が直接管理者・担当者に対策  
を指示することができ、対策の結果についても直接報告を受けることができるなど、  
大企業に比べて迅速に対応ができるという有利な条件を備えています。

また、この特  
質を生かすことで、大企業では必要となるセキュリティ監視や情報共有のための設備  
が不要とできるため、大企業よりも費用をかけずに対策を実現することも可能です。

##### 本書で用いてる語の説明

###### インシデント

###### （情報の）可用性

###### （情報の）完全性

###### （情報の）機密性

###### クラウドサービス

###### 個人情報

###### サイバーセキュリティ

###### CSIRT（ シーサート、Computer Security Incident Response Team）

###### 情報セキュリティ

###### 情報セキュリティインシデント

###### 情報セキュリティに関連した保険商品

###### 情報セキュリティポリシー

###### 情報セキュリティマネジメントサイクル

###### ソーシャルエンジニアリング

###### ランサムウェア

##### パブコメ段階

###### 付録 1 情報セキュリティ ５か条

ソフトウェアはつねに更新しよう

機器に応じたマルウェア対策をしよう

パスワードなど、認証を強化しよう

業務に使うすべてのサービスの設定を見直そう

脅威や攻撃の手口を知ろう

###### [付録 2 ５分できる！情報セキュリティ自社診断](http://www.ipa.go.jp/files/000054267.pdf)

Part 1 最重要事項

自社診断シートNo.1 ソフトウェアは常に最新の状態に更新

自社診断シートNo.2 マルウェア対策が提供されていれば導入

自社診断シートNo.3 推測されにくいパスワードを使用する

自社診断シートNo.4 すべてのサービスの設定を見直す

自社診断シートNo.5 脅威や攻撃に関する最新情報を集める

Part 2 ネットの脅威への対処

自社診断シートNo.6 電子メールは疑ってみる

自社診断シートNo.7 共有不可の電子メールアドレスはBCC に記入

自社診断シートNo.8 インターネットバンキングの偽サイトに注意する

自社診断シートNo.9 機器のパスワードは初期設定で使わない

自社診断シートNo.10 信頼できるクラウドを使う

Part 3 情報資産の保護

自社診断シートNo.11 社外保存データへのアクセス権に注意する

自社診断シートNo.12 バックアップを励行する

自社診断シートNo.13 秘密情報は安全な方法で持ち出す

自社診断シートNo.14 秘密情報は復元できないように消去する

自社診断シートNo.15 従業員の私物機器の業務での利用可否を決める

Part 4 職場のセキュリティ

自社診断シートNo.16 重要情報の放置を禁止する

自社診断シートNo.17 機器の盗難防止対策を講じる

自社診断シートNo.18 機器を勝手に操作させない

自社診断シートNo.19 見知らぬ人には声をかける

自社診断シートNo.20 オフィスの戸締まりに気を配る

Part 5 組織的対策事項

自社診断シートNo.21 従業員に守秘義務について理解してもらう

自社診断シートNo.22 従業員への定期的な教育・啓発を行う

自社診断シートNo.23 取引先にも秘密保持を要請する

自社診断シートNo.24 事故発生に備えて事前に準備する

自社診断シートNo.25 情報セキュリティ対策をルール化する

５分でできる自社診断シート

###### [付録 3 わが社の情報セキュリティポリシー](http://www.ipa.go.jp/files/000054268.pdf)

情報セキュリティポリシーは、外部のひな型をもってくるだけではうまく機能しません。企業の特徴に応じて中身を調整する必要があります。

ここでは、企業にどのような情報があるか、どのような脅威への対策が必要かをもとに情報セキュリティ診断に回答いただくと、情報セキュリティポリシーにどのような項目を盛り込む必要があるかがわかるようになっています。

手順１:情報資産管理台帳を作成して重要情報を確認

この付録で紹介している情報セキュリティポリシーは、情報資産管理台帳の作成を前提としています。企業で管理している情報を、＜ツール3-1＞のワークシートに書き出し、それぞれの重要度を判定してください。

また、それぞれの情報を管理している担当者を対象に、情報資産管理に関する役割を割り当てることになりますので、管理状況の実態についても正確に書き出すことが重要です。

手順２:警戒すべき脅威について確認

＜ツール3-２＞では、企業でIT機器やインターネット上のサービスなどを利用するときに警戒すべき脅威について紹介しています。

これをご一読いただいた上で、自社でも気になるものを選び、＜ツール3-３＞の「脅威」シートの該当欄に○印を記入してください。

なお、＜ツール3-２＞では機器の盗難など、以前から存在する脅威については紹介していませんが、脅威として想定する必要がないことを意味するわけではありませんのでご留意ください。

サブトピック 4

手順３:情報セキュリティ診断を実施

＜ツール3-３＞の「診断」シートを開き、現時点における自社の状況をもとに、項目ごとに以下から適切なものを１つ選択してください。

1: 実施している･･･対策を実施済みの場合, 2: 一部実施している･･･対策を実施しているが、十分でない場合, 3: 実施してない／わからない･･･対策を実施していないか、関連情報がない場合, 4: 自社には該当しない

手順４;必要なひな形を選んで編集すれば完成！

手順２と手順３が済むと、＜ツール3-３＞の「判定」シートに診断結果と自社で選択すべきひな型の一覧が表示されます。

＜ツール3-４＞からひな型をコピーし、自社の状況に反映するように編集（カスタマイズ）すれば、自社専用の情報セキュリティポリシーが完成します。

なお必要に応じて、さらに項目を追加していただいてもかまいません。

ツール 3-1 情報資産管理台帳

ツール 3-2 脅威一覧

ツール 3-3 対策状況チェックシート

ツール 3-4 情報セキュリティポリシー サンプル

###### [付録 4 情報セキュリティ関連ガイド・法令一覧](http://www.ipa.go.jp/files/000054273.pdf)

1. 1. 法令

1-1 個人情報保護法

1-2 マイナンバー法

1-3 不正競争防止法

1-4 不正アクセス禁止法

1-5 不正指令電磁的記録に関する罪

1-6 労働契約法

2. 2. ガイドライン

2-1 特定個人情報の適正な取扱いに関するガイドラン （事業者編）（個人情報保護委員会）

2-2 個人情報の 保護に関する法律ついての分野別 ガイドライン（各府省庁）

2-3 サイバーセキュリティ経営ガイドライン（経済産業省）

2-4 営業秘密管理指針（経済産業省）

2-5 秘密情報の保護ハンドブック（経済産業省）

2-6 組織における内部不正防止ガイドラン（IPA）

###### [付録 5 情報セキュリティ相談窓口](http://www.ipa.go.jp/files/000054274.pdf)

マルウェアに関する技術的な相談

標的型攻撃に関する相談

情報セキュリティに関する普及啓発の相談

Web改ざんやDoS攻撃に関する技術的な相談、攻撃元への調整依頼

不正アクセス／ウイルス感染による被害、事件性のあるもの、刑事罰対象の被害

#### ◦付録1：

##### [情報セキュリティ5か条（全2ページ、721KB）pdf](http://www.ipa.go.jp/files/000055516.pdf)

###### こんな情報があるはず！

従業員のマイナンバー、住所、給与明細

お客様や取引先の連絡先一覧

取引先ごとの仕切り額や取引実績

新製品の設計図などの開発情報

組織の経理情報

取引先から取扱注意と言われた情報

###### 漏れたら大変！こんなダメージが！

被害者への損害賠償などの支払い

取引停止、顧客の他社への流出

ネットの遮断などによる生産効率のダウン

従業員の士気低下

###### まずは始めてみよう

OSやソフトウェアは常に最新の状態に使用！

ウイルス対策ソフトを導入しよう！

パスワードを強化しよう！

共有設定を見直そう！

脅威や攻撃の手口を知ろう！

#### ◦付録2：

##### [5分でできる！情報セキュリティ自社診断シート（全2ページ、417KB）pdf](http://www.ipa.go.jp/files/000055517.pdf)

###### Part1 基本的対策

1.Windows Update※1 を行うなどのように、常にOS やソフトウェアを安全な状態にしていますか？

2.パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2 を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？

3,パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウェブサイトで使いまわしをしないなどのように、強固なパスワードを設定していますか？

4.ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、重要情報に対する適切なアクセス制限を行っていますか？

5.利用中のウェブサービス※3 や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？

###### Part2 従業員としての対策

6.受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？

7.電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？

8.重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？

9.無線LAN を利用する時は強固な暗号化を必ず利用するなどのように、無線LAN を安全に使うための対策をしていますか？

10.業務端末でのウェブサイトの閲覧やSNS への書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？

11.重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？

12.重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏えいを防止していますか？

13.重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？

14.離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？

15.事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？

16.退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？

17.最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？

18.重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？

###### Part3 組織としての対策

19.クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？

20.社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？

21.採用の際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？

22.情報管理の大切さなどを定期的に説明するなどのように、従業員に意識付けを行っていますか？

23.契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に秘密を守ることを求めていますか？

24.秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？

25.情報セキュリティ対策（上記1～24 など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？

###### ●さらなる情報セキュリティ対策の検討するには

「5 分でできる！情報セキュリティ自社診断」の次のステップとして、ガイドラインを活用したポリシーの策定やベンチマークでの自己診断を実施してみよう。

■ 中小企業の情報セキュリティ対策ガイドライン

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/>

■ 情報セキュリティ対策ベンチマーク

<https://www.ipa.go.jp/security/benchmark/>

###### ●自社診断シートで100 点満点を目指すには

「5 分でできる！情報セキュリティ自社診断パンフレット」のほか、以下のページで提供されている資料もより具体的な対策の検討に有用ですのでご活用ください。

■ 情報セキュリティ対策支援サイトiSupport

<https://www.ipa.go.jp/security/isec-portal/>

■ 対策のしおり

<https://www.ipa.go.jp/security/antivirus/shiori.html>

■ 映像で知る情報セキュリティ

<https://www.ipa.go.jp/security/keihatsu/videos/>

##### [情報セキュリティハンドブックひな形（全11ページ、444KB）PowerPoint](http://www.ipa.go.jp/files/000055529.pptx)

###### １ 全社基本ルール

OSとソフトウェアのアップデート

ウイルス対策ソフトの導入

パスワードの管理

アクセス制限

セキュリティに対する注意

独立行政法人情報処理推進機構（(略称：IPA）　重要なセキュリティ情報

<http://www.ipa.go.jp/security/index.html>

JVN （Japan Vulnerability Notes）

<http://jvn.jp/index.html>

一般社団法人 JPCERT コーディネーションセンター(略称：JPCERT/CC)

<https://www.jpcert.or.jp/>

###### ２ 仕事中のルール

電子メールの利用

インターネットの利用

データのバックアップ

クリアデスク・クリアスクリーン

重要情報の持ち出し

入退室

電子媒体・書類の廃棄

###### ３ 全社共通のルール

私有情報機器の利用

クラウドサービスの利用

###### ３ 従業員のみなさんへ

従業員の守秘義務

事故が起きてしまったら

#### ◦付録3：

##### [<ツールA>リスク分析シート（全5シート、79KB）excel](http://www.ipa.go.jp/files/000055518.xlsx)

###### 情報資産台帳記入例

###### 情報資産管理台帳

###### 脅威の状況

書類

秘密書類の事務所からの盗難

秘密書類の外出先での紛失・盗難

情報搾取目的の内部不正による書類の不正持ち出し

業務遂行に必要な情報が記載された書類の紛失

可搬電子媒体

秘密情報が格納された電子媒体の事務所からの盗難

秘密情報が格納された電子媒体の外出先での紛失・盗難

情報搾取目的の内部不正による電子媒体の不正持ち出し

業務遂行に必要な情報が記載された電子媒体の紛失

事務所PC

情報搾取目的の事務所PCへのサイバー攻撃

情報搾取目的の事務所PCでの内部不正

事務所PCの故障による業務に必要な情報の喪失

事務所PC内データがランサムウェアに感染して閲覧不可

不正送金を狙った事務所PCへのサイバー攻撃

モバイル機器

情報搾取目的でのモバイル機器へのサイバー攻撃

情報搾取目的の不正アプリをモバイル機器にインストール

秘密情報が格納されたモバイル機器の紛失・盗難

社内サーバー

情報搾取目的の社内サーバーへのサイバー攻撃

情報搾取目的の社内サーバーでの内部不正

社内サーバーの故障による業務に必要な情報の喪失

クラウド

安易なパスワードの悪用によるアカウントの乗っ取り

バックアップを怠ることによる業務に必要な情報の喪失

###### 対策状況チェック

(1) 組織的セキュリティ対策

経営者の主導で情報セキュリティの方針を示していますか？

情報セキュリティの方針に基づき、具体的な対策の内容を明確にしていますか？

情報セキュリティ対策を実施するための体制を整備していますか？

情報セキュリティ対策のためのリソース（人材、費用）の割当を行っていますか？

(2) 人的セキュリティ対策

秘密情報を扱う全ての者（パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員等を含む）に就業規則や契約等を通じて秘密保持義務を課していますか？

従業員の退職に際しては、退職後の秘密保持義務への合意を求めていますか？

会社の秘密情報や個人情報を扱うときの規則や、関連法令による罰則に関して全従業員に説明していますか？

(3) 情報資産管理

管理を必要とする情報資産は、すべて情報資産管理台帳に記載することを定めていますか？

秘密情報は業務上必要な範囲でのみ利用を認めていますか？

秘密情報の対象となるファイルやデータを丸秘マークや格付け表示等で識別可能とすることを定めていますか？

秘密情報を社外へ持ち出す時はデータを暗号化したり、パスワード保護をかけたりするなどの盗難・紛失対策を定めていますか？

秘密情報を机の上に放置せず施錠保管するなどして、のぞき見されたり紛失しないようにしていますか？

情報資産のバックアップに関する手順を定め、手順が遵守されていることを確認していますか？

秘密情報の入ったパソコンや紙を含む記録媒体を廃棄する場合、ゴミとして処分する前に、データの完全消去用のツールを用いたり、物理的に破壊したりすることで、データを復元できないようにすることを定めていますか？

(4) マイナンバー対応

特定個人情報の取扱ルール（管理担当者の割当て、関連規程の整備、記録の保存、定期的点検）が定められていますか？

特定個人情報に関する漏えい等の事案に備えた報告連絡体制が整備されていますか？

特定個人情報の保護のための安全管理措置（人的、物理的、技術的のそれぞれ）を行うことが定められていますか？

(5) アクセス制御と認証

業務で利用するすべてのサーバに対して、アクセス制御の方針が定められていますか？

サーバのアクセス権限は、従業員の退職や異動に応じて随時更新され、定期的なレビューを通じてその適切性が検証されていますか？

情報を社外のサーバ等に保存したり、グループウェアやファイル受渡サービスなどを用いたりする場合は、アクセスを許可された人以外が閲覧できることのないよう、適切なアクセス制御を行うことを定めていますか？

サーバで用いるパスワードは、適切なもののみが受け入れられる機能を通じて設定されていますか？

業務で利用する暗号化機能及び暗号化に関するアプリケーションは、その運用方針が明確に定められていますか？

(6) 物理的セキュリティ対策

業務を行う場所に、第三者が許可無く立入できないようにするための対策（物理的に区切る、見知らぬ人には声をかける、等）が講じられていますか？

最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？

高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？

秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？

(7) IT機器利用

セキュリティ更新を自動的に行うなどにより、常にソフトウェアを安全な状態にすることを定めていますか？

ウイルス対策ソフトウェアが提供されている製品については、用途に応じて導入し、定義ファイルを常に最新の状態にすることを定めていますか？

業務で利用するIT機器で用いるパスワードに関するルール（他人に推測されにくいものを選ぶ、機器やサービスごとに使い分ける、他人にわからないように管理する、等）ことを定めていますか？

業務で利用する機器が誰かに勝手に使われないようにするための措置（離席時にパスワード付きのスクリーンセーバーが動作する、持ち運び可能な機器は施錠できる場所に格納する、等）を定めていますか？

業務で利用するIT機器の設定について、不要な機能は無効にする、セキュリティを高める機能を有効にするなどの見直しを行うことを定めていますか？

社外で業務を行う場合のルールを定めていますか？

業務での個人所有機器の利用について、禁止しているか、利用する場合のルールを定めていますか？

受信した電子メールが不審かどうかを確認することを求めていますか？

電子メールアドレスの漏えい防止のためのBCC利用ルールを定めていますか？

インターネットバンキングやオンラインショップなどを利用する場合に偽サイトにアクセスしないための対策を定めていますか？

(8) IT基盤運用管理

IT機器と台帳との棚卸（実機確認）を行うとともに、社内ネットワークに許可なく接続された機器や無線LAN基地局がないことを確認していますか？

サーバで利用するアプリケーションは、ブラックリスト方式（利用してはいけないものを明示）またはホワイトリスト方式（利用してよいものを明示）のいずれかで特定していますか？

業務で利用するすべてのサーバに対して、脆弱性及びマルウェアからの保護のための対策を講じていますか？

サーバで用いた機器の廃棄の手順を定めていますか？

業務で利用するすべてのサーバやネットワーク機器に対して、必要性に応じてイベントログや通信ログの取得及び保存の手順を定めた上で、定期的にレビューしていますか？

サーバを対象とする監査を行うことを定めていますか？

ファイアウォールなど、外部からの攻撃の影響を防ぐための対策を導入していますか？

業務で使っているネットワーク機器のパスワードを初期状態のまま使わず、推測できないパスワードを設定して運用していますか？

クラウドサービスを利用する場合は、費用だけでなく、情報セキュリティや信頼性に関する仕様を考慮して選定していますか？

最新の脅威や攻撃についての情報収集を行い、必要に応じて社内で共有していますか？

(9) システム開発及び保守

情報システムの開発を行う場合、開発環境と運用環境とを分離していますか？

セキュアな開発を行うための手続きを定めていますか？

情報システムの保守を行う場合、既知の脆弱性が存在する状態で情報システムを運用しないようにするための対策を講じていますか？

(10) 外部委託管理

契約書に秘密保持（守秘義務）、漏洩した場合の賠償義務、再委託の制限についての項目を盛り込むなどのように、委託先が遵守すべき事項について具体的に規定していますか？

委託先との秘密情報の受渡手順を定めていますか？

委託先に提供した秘密情報の廃棄または消去の手順を定めていますか？

(11) 情報セキュリティインシデント対応ならびに事業継続管理

秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故の発生に備えた準備をしていますか？

インシデントの発生に備えた証拠情報の収集手順を定め、運用していますか？

事業継続計画における情報セキュリティ対策を定めていますか？

###### 診断結果

##### [<ツールB>情報セキュリティポリシーサンプル（全50ページ、159KB）](http://www.ipa.go.jp/files/000055794.docx)

### [•中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 【パブリックコメント中】](http://www.ipa.go.jp/security/keihatsu/sme/guideline/)

#### [◦「中小企業の情報セキュリティ対策ガイドライン改訂版](http://www.ipa.go.jp/files/000054275.pdf)

#### [◦付録1　情報セキュリティ5か条](http://www.ipa.go.jp/files/000054266.pdf)

#### [◦付録2　5分でできる！情報セキュリティ自社診断](http://www.ipa.go.jp/files/000054267.pdf)

#### [◦付録3　わが社の情報セキュリティポリシー](http://www.ipa.go.jp/files/000054268.pdf)

#### [◦付録3　わが社の情報セキュリティポリシー（ツール3-1　情報資産管理台帳）](http://www.ipa.go.jp/files/000054269.pdf)

#### [◦付録3　わが社の情報セキュリティポリシー（ツール3-2　脅威一覧）](http://www.ipa.go.jp/files/000054270.pdf)

#### [◦付録3　わが社の情報セキュリティポリシー（ツール3-3　対策状況チェックシート）](http://www.ipa.go.jp/files/000054271.pdf)

#### [◦付録3　わが社の情報セキュリティポリシー（ツール3-4　情報セキュリティポリシーサンプル）](http://www.ipa.go.jp/files/000054272.pdf)

#### [◦付録4　情報セキュリティ関連ガイド・法令一覧](http://www.ipa.go.jp/files/000054273.pdf)

#### [◦付録5　情報セキュリティ相談窓口](http://www.ipa.go.jp/files/000054274.pdf)

### サイバーセキュリティ経営ガイドライン

### 企業経営のためのサイバーセキュリティの考え方

### その他

#### [中小企業に特化した情報セキュリティ対策の相談対応【私見】 - CyberSec diary](#_________________________________CyberSec_diary_2)

#### [•中小企業経営者向けセキュリティ対策情報のレファレンスリスト - CyberSec diary](#__________________________________CyberSec_diary_2)

#### [•中小企業に特化した情報セキュリティ対策の相談対応 - CyberSec diary](#_____________________________CyberSec_diary_4)

#### [•中小企業のサイバーセキュリティ対策インデックス（経営者・管理者・従業員） - CyberSec diary](#_________________________________________CyberSec_diary_2)

## 家庭個人向け

### [•家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec diary【更新中】](#___________________________CyberSec_diary______2)

## 重要インフラ関連

### [•重要インフラ・大企業向けサイバーセキュリティ対策 - CyberSec diary【更新中】](#_____________________________CyberSec_diary______2)

## 政府機関等向け

### [政府機関向けサイバーセキュリティ対策 - CyberSec diary【更新中】](#______________________CyberSec_diary_______)

## 情報セキュリティマネジメント関連

### [•サイバーセキュリティとは - CyberSec diary](#_________________CyberSec_diary_2)

### [•情報セキュリティに関する基礎知識 - CyberSec diary](#_____________________CyberSec_diary_2)

### [•情報セキュリティ対策の概念 - CyberSec diary](#__________________CyberSec_diary_2)

### [•情報セキュリティポリシー、実施手順 - CyberSec diary](#______________________CyberSec_diary_2)

### [•情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary](#__________________________________________CyberSec_diary_2)

### [•セキュリティインシデント対応は事業継続計画（BCP）の一つ - CyberSec diary](#________________________BCP_______CyberSec_diary_2)

## 人材育成・人材確保

### [•小規模サイトにおける情報システム担当者が持つべき知識とスキル - CyberSec diary](#___________________________________CyberSec_diary_2)

### [•情報セキュリティマネジメントに必要な知識 - CyberSec diary](#_________________________CyberSec_diary_2)

## 関連基準、法規、対策機関等

### [•サイバーセキュリティに関連したガイドライン等インデックス - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_guide_index)

#### ◦公的機関、教育機関向け、個人ユーザー向け、事業者向け

### [•政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec diary](#_____________________________26_______CyberSec_diary_2)

#### ◦全体的内容、規定の趣旨、対策例

### [•情報セキュリティ関連法規リスト（更新中） - CyberSec diary](#_________________________CyberSec_diary_4)

### [•サイバーセキュリティ対策公的機関・関連団体・関連機関インデックス - CyberSec diary](#_____________________________________CyberSec_diary_2)

## セキュリティ関連情報提供サイト一覧

### [•サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポータルサイト - CyberSec diary](#__________________________________________CyberSec_diary_4)

## ニュース

### [•中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 【パブリックコメント中】](#___________________________IPA______________________________3)

### [•「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec diary](#______________________________CyberSec_diary_2)

# [緊急対応時のピックアップ情報](http://cybersec.hatenadiary.jp/entry/top)

# [情報セキュリティが心配になったら - CyberSec diary](http://cybersec.hatenadiary.jp/entry/top)

## 【緊急】どんな環境で何が起きてますか？まずは落ち着いて今起きている事象を確認しましょう

### [•セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式)](http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf)

#### ◦セキュリティの専門家へ相談する際に事前に確認しておいてほしいこ とを問診票の形式でまとめたもの。漠然とした不安の中で相談をする際に、今自分や企業がどういった状況にあるのかを見直し、不安の原因を確認し、スムーズに相談を進めることができます。

## 【緊急】セキュリティ侵害の可能性があるが、どこに問い合せていいかわからない?

### [•「中小企業サイバーセキュリティ対策相談窓口」へ](http://cybersec.hatenadiary.jp/entry/2016/06/25/131046)

#### ◦☎ 03-5320-4773

## 【緊急】情報の漏えい・改ざんが起きている？

### •犯罪の可能性がある場合は、警視庁へ

#### ◦サイバー犯罪に係る電話相談

##### ☎ 03-3431-8109

##### [情報セキュリティ広場](http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html)

##### [警察署一覧 警視庁](http://www.keishicho.metro.tokyo.jp/about_mpd/shokai/ichiran/index.html)

## 【緊急】PC、スマホの動きがおかしくなった、データが壊れた?

### •ウイルス感染、不正アクセスの可能性

#### ◦IPAセキュリティセンター　「情報セキュリティ安心相談窓口」

##### ☎ 03-5978-7509 e-mail anshin@ipa.go.jp

##### [「情報セキュリティ安心相談窓口」](https://www.ipa.go.jp/security/anshin/)

## 【緊急】実被害にあった場合

### •同様の被害を拡大させないためにも、速やかに届けてください。

### •ウイルス・不正アクセス届出

#### [◦IPAセキュリティセンター](https://www.ipa.go.jp/security/)

##### ☎03-3518-2177

### •インシデント報告・届出

#### [◦JPCERT コーディネーションセンター](https://www.jpcert.or.jp/)

##### ☎03-3518-2177

### •サイバー犯罪届出（全国）

#### [◦「警察庁　サイバー犯罪対策」](https://www.npa.go.jp/cyber/)

##### [◦都道府県警察本部のサイバー犯罪相談窓口等一覧](https://www.npa.go.jp/cyber/soudan.htm)

## 【相談】セキュリティ関連の各種相談、問合せ

### •嫌がらせ、ネットストーカーの相談

#### ◦管轄の警察署の生活安全課

#### [警察署一覧（警視庁）](http://www.keishicho.metro.tokyo.jp/about_mpd/shokai/ichiran/)

### •ECサイトのなりすまし被害

#### [◦なりすましECサイト対策協議会](https://www.saferinternet.or.jp/narisumashi/)

#### [「なりすましECサイト対策マニュアル」（PDF, 928KB）](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)

## 【一般】セキュリティに限らず、消費生活全般に関する苦情や問合せ先は？

### [•消費者ホットライン](http://www.caa.go.jp/region/shohisha_hotline.html)

#### ☎188

### •暮らしにかかわる東京都の情報サイト

#### [◦東京都の消費生活総合サイト 東京くらしWEB](http://www.shouhiseikatu.metro.tokyo.jp/)

#### [◦消費生活相談窓口のご案内 | 東京くらしWEB](http://www.shouhiseikatu.metro.tokyo.jp/sodan/sodan.html)

## 【事前予防】情報セキュリティ侵害に遭わないように事前に対処しておきましょう

### •情報セキュリティ対策の基本を知る

#### [◦情報セキュリティ対策９カ条【NISC,IPA】(pdf形式)](http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf)

##### インターネットを安全に利用するための最低限の対策を記載したリーフレットです

#### •情報セキュリティに関する脅威を知る

##### [◦10大脅威2016簡易説明資料（個人編）(PDF形式 4.79MB)](https://www.ipa.go.jp/files/000052127.pdf)

##### [◦10大脅威2016簡易説明資料（組織編）(PDF形式 4.67MB)](https://www.ipa.go.jp/files/000052128.pdf)

##### [◦10大脅威2016簡易説明資料（総合編）(PDF形式 6.02MB)](https://www.ipa.go.jp/files/000052126.pdf)

## 【知識】情報セキュリティ対策の必要性を認識し、網羅的な対策を知るには？

### [•中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構](http://www.ipa.go.jp/security/keihatsu/sme/guideline/)

#### ◦中小企業に求められる情報セキュリティ対策を、中小企業ならではの視点から体系的に実現するための方策が紹介されている。

### •教育・学習（企業・組織向け）｜ここからセキュリティ！ 情報セキュリティ・ポータルサイト

#### ◦情報セキュリティ対策に関して有用な情報を体系的に提供しているサイト

### [•企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】(pdf形式)](http://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)

#### ◦これから情報セキュリティ対策を実施していこうと考えている企業(組織)の経営者(運営者)、管理者、従業者の方を対象と想定しています。 情報セキュリティ対策の見直し、委託先や子会社に対するセキュリティ教育のための参考資料としても活用できます。

## 参考情報

### 信頼性の高いセキュリティ対策情報を提供しているサイトの内容を解説します

#### [•ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【相談事例集作成候補】 - CyberSec diary【ページ内検索用】](http://cybersec.hatenadiary.jp/entry/kokokara_case)

##### 1ページ内に全リンクを表示し、その内容によってレベル表示をし、また必要に応じで内容の解説を加えたもの。

### 中小企業向けサイバーセキュリティ関連ニュース

#### [「中小企業サイバーセキュリティ対策相談窓口」の開設及び「東京中小企業サイバーセキュリティ支援ネットワーク」の設立(2016年4月25日)](http://cybersec.hatenadiary.jp/entry/2016/06/25/131046)

#### [•東京都の中小企業対策に関する重点要望（2016年5月12日, 東京商工会議所）](https://www.tokyo-cci.or.jp/file.jsp?id=79482)

#### [•東京都の中小企業サイバーセキュリティ支援ネットワーク Tcyss (ティーサイス) に参画 – 日本のセキュリティチーム（2016年8月9日, 日本マイクロソフト）](https://blogs.technet.microsoft.com/jpsecurity/2016/08/09/tcyss/)

#### [•東京中小企業サイバーセキュリティ支援ネットワーク(Tcyss) 警視庁 （2016年9月26日, 警視庁）](http://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/tcyss.html)

## 他のページへのリンク

### [中小企業サイバーセキュリティ対策関連の備忘録 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/index)

# [•サイバーセキュリティ相談・届出先クイックリスト - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_consul_quick_guide)

## 凍結中

# [•情報セキュリティ緊急対応ガイド【汎用】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_emergency_response_guide)

## ■緊急対応（自然災害, 大火災, 感染症, テロ, , ,）

### 事象の検知、報告受付(Detect)

### 事実確認、対応の判断 被害の局所化(拡大防止)(Triage)

#### ◦該当システムをただちにネットワークから切り離し、使用を中止する。

#### ◦被害の範囲を確認し、使用を停止する

### 緊急連絡

#### ◦システム管理者、関係部署、関係機関に連絡。指示に従う。

#### ◦犯罪の可能性⇒警視庁

#### ◦ウイルス、不正アクセス被害届出⇒IPAセキュリティセンター

### 原状保全

#### ◦原因調査のためにサーバ、PC内のファイルをバックアップし保存する

### 原因調査

#### ◦なぜ情報セキュリティ侵害が起きたか？

#### ◦サーバ、PC内のファイルに改ざんされたものがないか、本来存在しないファイルがないかを確認する

#### ◦サーバのログ等を確認して、通常でないファイル転送、アクセス等を確認する。

### 早期復旧・事業継続 (Respond)

#### ◦確認できた事象に対する再発防止のための改善策を、システム管理者の指示に従って、適切な復旧を行う。

### 恒久的対策（再発防止策）

#### ◦インシデントからの知見の学習

#### ◦ルールの再確認

##### 事業継続計画、情報セキュリティポリシー

##### 緊急時対応、人的、管理的、物理的、技術的対策の内容の確認と是正

###### 情報セキュリティ侵害の原因の多くが、人為的なミスもしくは悪意によるもの。

###### 最低限守るべきルールを明確にして、それを守らせることが重要。

### 通常運用

#### ◦平時からの実施状況の確認（監査）

## ■情報セキュリティ対策の必要性

### •ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、セキュリティ侵害、、）が発生して、事業資産（人・もの（情報及び設備）・金）、社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性がある。

### •どんな緊急事態が発生しても、事業を継続できるようにする対策を明示しておくことが必要

### •情報セキュリティ対策は、事業継続計画の一つ

### •サービスの向上を図るために、情報資産（保有情報（媒体に依らず）、情報機器、情報システム）に対する情報セキュリティ上のリスクを低減させる

### •ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用の中で実施すべき先行投資であり、緊急事態が発生した後に対処する経費として想定してはいけない

## ■情報セキュリティ対策の基本

### 情報セキュリティ侵害とは

#### ◦機密性、完全性、可用性が損なわれること

#### ◦全ての人は当事者

##### 誰しも被害者になる。また、知らぬうちに加害者にもなる

### [脅威・手口を知る（10大脅威2016簡易説明資料（組織編））](https://www.ipa.go.jp/files/000052128.pdf)

#### ◦人的脅威

##### 不注意

###### メール添付ファイルを開ける、偽サイトへのアクセス

###### PC、USBの紛失

##### 内部者によるセキュリティ侵害

###### 情報の持ち出し、不正アクセス

#### ◦正規のウェブサイトを改ざん

#### ◦ウェブサイトにアクセスするだけでマルウェア感染

#### ◦標的型メールでの不正サイトへの誘導

#### ◦不審なメールのマルウェア添付

### 情報資産の認識

#### ◦取り扱われる情報資源の格付け（機密性、完全性、可用性が損なわれた場合の経済的、社会的損害の大きさ）のレベル等に応じた重要度を認識する

### リスク分析

#### ◦リスク＝情報資産に対する脅威（侵害する行為の発生頻度）×情報資産の重要度（機密性レベル＋完全性レベル＋可用性レベル）×脆弱性（実際に侵害が起きる可能性）

### 対策はリスクの高いものを優先する

#### ◦どれだけコストをかけてもリスクをゼロにすることは困難であり、脅威の大きさ、情報資産の重要性、脆弱性の大きさを勘案し、不必要に過度な対策とならないように検討する

#### ◦重要度の高いファイルのバックアップ

#### ◦ソフトウェアの更新

#### ◦マルウェア（ウイルス等）対策ソフトの導入

#### ◦パスワード・認証の強化

#### ◦設定の見直し（ルータ、PC等）

### 恒久的対策

#### ◦定期的なバックアップ

##### ランサムウェア等を含めた対策

##### バックアップ媒体は、取得後、ネットワークから切り離す

#### ◦ルールの策定

##### 事業継続計画（BCP）の策定

##### 情報セキュリティポリシーの策定

##### 人的、管理的、物理的、技術的対策

#### ◦フールプルーフ対策

##### 人間が間違えても危険にならない仕組みにしておく

#### ◦フェールセーフ対策

##### 機械が壊れても危険にならない仕組みにしておく

#### ◦ルールの遵守

##### 情報セキュリティポリシーの遵守

##### [実施手順の遵守（情報セキュリティ対策９カ条）](http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf)

###### OSやソフトウェアは常に最新の状態に

###### パスワードは貴重品のように管理

###### ログインID・パスワードは絶対に教えない

###### 身に覚えのないファイルは開かない

###### ウイルス対策ソフトを導入

###### ネットショッピングは信頼できるお店で

###### 大切な情報は失う前に複製

###### 外出先では紛失・盗難に注意

###### 困ったときは一人で悩まず相談を

### 定期的な監査

## ■参考資料

# [•相談対応の手引きレファレンスリスト【相談員用】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/response_guidance_ref)

## ■信頼性の高いセキュリティ対策情報を提供しているサイトの内容の解説

### [•ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/kokokara_case)

#### [◦「ここからセキュリティ！」のサイト内情報を検索・選択しやすいように、1ページ内に全リンクを表示し、その内容によってレベル表示をし、また必要に応じで内容の解説を加えたもの。](http://www.ipa.go.jp/security/kokokara/)

#### ◦検索の際はWebブラウザの検索機能を利用してください

## ■事例等の紹介

### [•セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_shingai_case_site)

## ■対策まとめ資料

### •情報セキュリティ対策とは

#### [◦情報セキュリティに関する基礎知識 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_prime_kb)

#### [◦事業継続計画（BCP）とセキュリティインシデント対応](http://cybersec.hatenadiary.jp/entry/2016/06/29/151025)

#### [◦情報セキュリティ対策の概念 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_response_concept)

#### [◦情報セキュリティポリシー、実施手順 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_policy)

### •中小企業向け対策

#### [◦中小企業に特化した情報セキュリティ対策の相談対応 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_consul_response)

#### [◦中小企業の現状から見た対策の考え方【私見】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_response_shiken)

### •システム調達におけるセキュリティ要件定義

#### [◦情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/it_chotatsu_sec_response)

### ――――――――相談対応の手引き用【更新中】――――――

#### [【更新中】情報セキュリティ緊急対応ガイド【汎用】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_emergency_response_guide)

#### [•【更新中】サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_sodan_tebiki_memo)

# [•サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_sodan_tebiki_memo)

## •サイバーセキュリティ対策相談対応の手引き（メモ）

### 展開した文書

# [•セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_shingai_case_site)

## 各種Webから抜粋したページ

## [◦相談窓口対応事例（FAQ候補） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/tcyss_faq_Candidate)

# [•ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/kokokara_case)

## 「ここからセキュリティ」を展開したページ

# [•IT化・デジタル化により業務の効率化・サービスの向上を図るために、セキュリティ対策を実施【私見】](http://cybersec.hatenadiary.jp/entry/chusho_response_shiken)

## ■デジタルトランスフォーメーション時代の情報セキュリティ対策

### ●IT活用の必然性と情報セキュリティ対策の必要性

#### •デジタルトランスフォーメーションとは、

##### ◦組織をデジタルの世界に移行させる変化

###### 旧態依然のサービスを捨てて、テクノロジーの進展と共に常に変化し続けるビジネス・モデルを受け入れる時代

##### ◦人やものがデジタルデータで直接繋がり、時空間の制約なく、「業種業態の枠を越えた」新たな仕組みを作り出せる時代の変化

###### 形を変革、再編成により、既存の事業にない「デジタルビジネス」が登場しつつある。

##### ◦「デジタル・トランスフォーメーション」によりサービス化、オープン化、ソーシャル化、スマート化の4つの大きな変化が生まれつつある。

##### ◦現代のデジタルネイティブなユーザをターゲットとしたビジネスモデルやビジネスプロセスの変革

#### •デジタルトランスフォーメーションの効果、

##### ◦業界・業種を越えた企業が連携し、新たなビジネスやサービスを創出していく原動力となりつつある。

##### ◦グローバルビジネスの世界に新たな競争原理をもたらそうとしている。

##### ◦中小企業において

###### デジタル化の進展を受入れ、それを活用して顧客との関係性強化を図る企業にとっては、大きなビジネスチャンスが到来している。

###### 柔軟にかつ大企業に先駆けて、デジタルトランスフォーメーションに対応していくことが、組織の発展につながる。

#### •今まで

##### ◦これまで企業のITシステムは、業務、生産工程等を効率化して、経営を安定化させることに重きが置かれてきた。

##### ◦単なる効率化だけではビジネスの競争に勝ち残れない

##### ◦従来型のサービスはしばらくは継続できるかもしれないが、デジタルの未来に移行し始めなければ、もう生き残ることができない

##### ◦現在、必要とされているのがデジタルトランスフォーメーションによる大胆かつ、スピーディーな変革が発展への道

#### •今後

##### ◦従来から業務の改善のために情報化が進められてきたが、今後はDigital Transformation時代に、如何にIT、デジタル情報を戦略的に活用できるかが問われる

##### ◦サービスの向上、サービスの継続、事業の効率化のために、デジタル化した情報をITによって利活用し、高付加価値の新たなサービスに変遷していく。

#### •情報セキュリティ対策の必要性

##### ◦しかし、ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、セキュリティ侵害、、）が発生して、事業資産（人・もの（情報及び設備）・金）、社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性がある。

##### ◦どんな緊急事態が発生しても、事業を継続できるようにする対策を明示しておくことが必要

##### ◦情報セキュリティ対策は、事業継続計画の一つ

##### ◦サービスの向上を図るために、情報資産（保有情報（媒体に依らず）、情報機器、情報システム）に対する情報セキュリティ上のリスクを低減させる

##### ◦ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用の中で実施すべき先行投資であり、緊急事態が発生した後に対処する経費として想定してはいけない

#### •情報システムの構築において

##### ◦即時性が要求されるサービスや提供するサービス内容の多様化・複雑化等に対応するために、業務手続の標準化と徹底した電子化の推進、情報セキュリティ上の要件を満たす前提での外部委託の活用、他業務業態のシステムとの連携等を検討する

### セキュリティ侵害の実態

#### •「個人情報漏えい」原因の比率上位5位（2013年　NPO日本ネットワーク協会）

##### ◦・誤操作34.9%

##### ◦・管理ミス32.3%

##### ◦・紛失・置忘れ14.3%

##### ◦・盗難5.5%

##### ◦・不正アクセス4.7%

#### •個人情報漏えい媒体、経路（2013年　NPO日本ネットワーク協会）

##### ◦・紙媒体58.7％

##### ◦・USB等記憶媒体25.9％

##### ◦・電子メール5.5％

##### ◦・インターネット5.0％

### 情報セキュリティ対策の必要性の認識が必要

#### •被害にあった場合、影響が如何に大きいかを認識する⇒事例に基づいた被害と対策の必要性の認識が必要。

##### セキュリティ侵害事象は対岸の火事ではない

##### 一度セキュリティ侵害を受けると、社会的信用、経済的被害により、事業継続が困難になる

#### •☆セキュリティ対策の目的は、

##### IT化、デジタル化は、業務の効率化、ITを使ったサービスの向上

###### どんな優れたサービスも、セキュリティに不安があるサービスは利用されない

##### ◦ITを活用するために、セキュリティ対策を実施

###### （自動車を運転するために、自動車保険に入る）

##### ◦セキュリティ侵害の影響を認識する

###### 機密性（個人情報、取引先の情報、知的財産）、預金残高

###### 完全性（Webページ、帳簿類）

###### 可用性（業務システム、サービスシステム）

##### ◦費用対効果を考える

###### 対策に要する費用と、侵害にあった場合の被害の大きさを比較する

自動車任意保険、火災保険のようなもの。

また、自動車のレーダー探知機とかも⇒監視することにより抑止効果もあり

###### 守るべき資産に応じてリスクの高いものから優先的に対応することにより、少ないコストで大きな効果が得られる

どれだけ費用をかけて対策をしてもリスクは0にならない。

最も大きなリスク要因は「人」であり、ルールの策定と遵守が最も効果が大きい

##### ◦事業継続の観点で

###### 経済的損失、社会的信用の喪失⇒事業存続、事業継続の危機

### システムをベンダーに任せて開発もしくは導入、運用している

#### •セキュリティ対策を明確にした調達仕様書作成のスキル習得が必要

### 効果的な情報セキュリティ対策の方法がわからない

#### •認識すること

##### ◦断片的な対策では、セキュリティホールはなくならない

##### ◦内部職員による故意もしくは過失によるセキュリティ侵害は全体の80％以上

##### ◦どれだけお金を掛けても脆弱性はゼロにはならない

##### ◦リスク（脅威×資産価値×脆弱性）の高いものから順次対策を講ずる

#### •守るべき情報資産を洗い出して、管理的、技術的、人的、物理的対策の個別の対策の検討方法をレクチャー⇒情報セキュリティマネジメントシステム（ISMS）に準拠した情報セキュリティ対策の考え方

# [•デジタルトランスフォーメーション時代のITとデジタル情報の活用 - CyberSec diary　【作成中】](http://cybersec.hatenadiary.jp/entry/digital_trans_IT_util)

## 【作成中】

## ■活用戦略

## ■活用技術

## ●クラウドコンピューティング

# [中小企業に特化した情報セキュリティ対策の相談対応【私見】 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_consul_response)

## 対象範囲と役割分担

## 中小企業の現状

### •組織の意識と対策

#### ◦情報セキュリティ対策の必要性の認識が低い

##### 被害にあった場合、影響が如何に大きいかを認識させる⇒事例に基づいた被害と対策の必要性の啓発。

#### ◦システムをベンダーの言いなりで開発もしくは導入、運用

##### セキュリティ対策を明確にした調達仕様書のためのスキル教育の方法をレクチャー

#### ◦情報セキュリティ対策の方法がわからない

##### 守るべき情報資産を洗い出して、管理的、技術的、人的、物理的対策の個別の対策の検討方法をレクチャー⇒情報セキュリティマネジメントシステム（ISMS）に準拠した情報セキュリティ対策の考え方

### •実態調査

#### 意識レベル 意識がない⇒啓発から、意識がある⇒具体的な対策から

#### セキュリティ対策レベル【仮定】

##### LEVEL0 ITパスポート試験レベルの担当者もいない

##### LEVEL1 ITパスポート試験レベルの担当者がいる

##### LEVEL2 情報セキュリティマネジメント試験レベルの担当者がいる

##### LEVEL3 応用情報処理技術者試験レベルの担当者がいる

#### システムの内部調達・外部委託別

##### 要件定義はどちらでも

##### 外部委託は、調達仕様書が作成できるスキルの有無

##### 内部調達は、情報セキュリティ

##### スペシャリストレベルのスキルを持った設計開発者

## 中小企業への支援

### •普及啓発

#### ◦対策の必要性、対策概要、具体的な対策

##### システムを使った事業の実施、創業のためには、情報セキュリティ対策が必要である

##### セキュリティ対策は、経費でなく、システム構築の一要件であり将来への投資であることを理解してもらう

#### ◦啓発内容の例

##### セキュリティ侵害の事例

###### 脅威の事例

###### リスクの事例

##### セキュリティ対策の事例

###### 費用対効果の高い対策とは

###### システムを構築する際の対策

###### 情報セキュリティ侵害があった時の対策

### •対策の概要

#### ◦セキュリティ対策の普及啓発

##### ⇒啓発用Webページ、セミナー等の案内

###### 連携機関でのセミナー開催予定

###### 他機関でのセミナー開催予定

#### ◦セキュリティの予防対策

##### システム化構築のPDCAサイクル

###### 脆弱性を低減するシステム企画・設計構築

###### セキュリティ侵害が発生したときに、速やかに対応できる運用、保守

##### 過剰、過小な対策を防ぐ提案

###### ⇒情報セキュリティ対策を含めたBCPの策定を提案

###### ⇒情報セキュリティに特化した対策はISMSの体系に沿った対策を提案

##### 重大事象を優先的に対策 重要の情報資産は何か

###### 重要な情報資産への頻度の高い脅威の洗い出し

###### 脅威に対する脆弱性の度合い

###### 脆弱性を低減させる対策は？

#### ◦セキュリティ侵害の事象発生（インシデント）の可能性あり

##### 段階

###### セキュリティ侵害の予兆段階

###### セキュリティ侵害の発生

##### 案内先

###### 犯罪の可能性

###### 一般的な不正アクセス、ウイルス感染

###### 高度な技術的対策が必要な事象

# [•中小企業経営者向けセキュリティ対策情報のレファレンスリスト - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_response_ref)

## ■緊急相談対応

### •サイバーセキュリティ相談・届出先クイックリスト - CyberSec diary

#### ◦セキュリティ相談の受付内容により、具体的な対応先へ的確に案内するためのクイックリスト

### •セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式)

#### ◦セキュリティの専門家へ相談する際に事前に確認しておいてほしいこ とを問診票の形式でまとめたものである。漠然とした不安の中で相談をする際に、今自分や企業がどういった状況にあるのかを見直し、不安の原因を確認し、スムーズに相談を進めることができることを目的としている。

### •情報セキュリティに関する基礎知識 - CyberSec diary

#### ◦情報セキュリティ対策の基本、情報セキュリティ 10 大脅威（個人）、情報セキュリティ 10 大脅威（組織）、注目すべき脅威や懸念、サービス提供と情報セキュリティ対策

#### 

#### ◦10大脅威2016【IPA】

##### 10大脅威2016簡易説明資料（総合編）(PDF形式 6.02MB)

##### 立場ごとのTop5を抜粋した簡易説明資料

###### 10大脅威2016簡易説明資料（個人編）(PDF形式 4.79MB)

###### 10大脅威2016簡易説明資料（組織編）(PDF形式 4.67MB)

##### 【参考】

##### 詳細資料：情報セキュリティ10大脅威 2016(PDF形式 3.95MB)

##### 2アップ印刷用（用紙1枚に2ページ分を印刷）はこちら

#### ◦情報セキュリティ対策９カ条【NISC,IPA】(pdf形式)

##### インターネットを安全に利用するための最低限の対策を記載したリーフレットです。

### •情報セキュリティ緊急対応ガイド– CyberSec diary

#### ◦緊急対応の段階と、情報セキュリティ対策の基本要件

## ■中小企業経営者向け情報

### •情報セキュリティ対策９カ条【NISC,IPA】(pdf形式)

#### ◦インターネットを安全に利用するための最低限の対策を記載したリーフレットです。

### •5分でできる！情報セキュリティポイント学習【オンライン】【ダウンロード】【IPA】

#### ◦1テーマ5分で情報セキュリティについて勉強できる学習ツールです。あなたの職場の日常の1コマを取り入れた親しみやすい学習テーマで、セキュリティに関する様々な事例を疑似体験しながら正しい対処法を学ぶことができます。日頃のセキュリティ対策の確認にご活用ください。

### •企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】(pdf形式)

#### ◦これから情報セキュリティ対策を実施していこうと考えている企業(組織)の経営者(運営者)、管理者、従業者の方を対象と想定しています。 情報セキュリティ対策の見直し、委託先や子会社に対するセキュリティ教育のための参考資料としても活用できます。

### •中小企業のためのセキュリティツールライブラリ一覧【IPA】

#### ◦セキュリティテーマと内容レベルから最適ツールを選べます。 ツールを「現状把握」「対策・立案」「効果測定」「改善・見直し」の4テーマに分類。さらに内容に応じて「初級」「中級」「上級」の3レベルに分けて小冊子が用意されています。 あなたの会社のセキュリティテーマや求めている内容レベルに合致したツールを選んで効果的にご利用ください。

### •その他の各種情報へのリンク

#### ◦情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary

## ■家庭・個人向け情報

### •【準備中】

## ■サイバーセキュリティ対策公的機関・関連団体・関連機関

### •サイバーセキュリティ対策公的機関・関連団体・関連機関インデックス - CyberSec diary（準備中）

## ■体系的・網羅的な情報を提供しているポータルサイト

### •サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポータルサイト - CyberSec diary

## ■人材育成・人材確保

### •小規模サイトにおける情報システム担当者が持つべき知識とスキル - CyberSec diary

### •情報セキュリティマネジメント -- XMind Online Library

## ■参考情報

### •サイバーセキュリティに関連したガイドライン等インデックス - CyberSec diary

#### ◦公的機関、教育機関向け、個人ユーザー向け、事業者向け

### •情報セキュリティ関連法規リスト（更新中） - CyberSec diary

### •政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec diary

## ■関連ニュース

## ―――――― 相談対応の手引き用 ―――――

### ■信頼性の高いセキュリティ対策情報を提供しているサイトの内容の解説

#### •ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【相談事例集作成候補】 - CyberSec diary

##### ◦「ここからセキュリティ！」のサイト内情報を検索・選択しやすいように、1ページ内に全リンクを表示し、その内容によってレベル表示をし、また必要に応じで内容の解説を加えたもの。

##### ◦検索の際はWebブラウザの検索機能を利用してください

### ■事例等の紹介

#### •セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec diary

### ■対策まとめ資料

#### •情報セキュリティ対策とは

##### ◦情報セキュリティに関する基礎知識 - CyberSec diary

##### ◦セキュリティインシデント対応は事業継続計画（BCP）の一つ - CyberSec diary

##### ◦情報セキュリティ対策の概念 - CyberSec diary

##### ◦情報セキュリティポリシー、実施手順 - CyberSec diary

#### •中小企業向け対策

##### ◦中小企業に特化した情報セキュリティ対策の相談対応 - CyberSec diary

##### ◦中小企業の現状から見た対策の考え方【私見】 - CyberSec diary

#### •システム調達におけるセキュリティ要件定義

##### ◦情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary

## ――――――――相談対応の手引き用【更新中】――――――

### 【更新中】

#### サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec diary

# [•中小企業に特化した情報セキュリティ対策の相談対応 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_consul_response)

## ■対象範囲と役割分担

## ■中小企業の現状

## ■中小企業への支援

# [•中小企業のサイバーセキュリティ対策インデックス（経営者・管理者・従業員） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_sec_responce_index)

## ■サイバーセキュリティ対策の必要性

### •情報セキュリティの脅威

### •守るべき情報資産の認識

### •最低限の対策

## ■理解度確認

## ■対策のしおり

## ■中小企業のサイバーセキュリティ対策にフォーカスした体系的・網羅的な情報

### ※主なサイトへのリンク

## ■個人のサイバーセキュリティ対策にフォーカスした体系的・網羅的な情報

### ※主なサイトへのリンク

# [•家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec diary【更新中】](http://cybersec.hatenadiary.jp/entry/home_response)

## 更新中

# [•重要インフラ・大企業向けサイバーセキュリティ対策 - CyberSec diary【更新中】](http://cybersec.hatenadiary.jp/entry/daikigyo_response)

## 重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ（案）【NISC】

### <http://www.nisc.go.jp/conference/cs/dai07/pdf/07shiryou02.pdf>

## サイバーセキュリティ経営ガイドライン【2016年12月METI】

### サイバーセキュリティ経営ガイドラインVer 1.1【2016年12月METI】

#### <http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v1.1.pdf>

### サイバーセキュリティ経営ガイドライン Ver1.1（Ver1.0との差分）【2016年12月METI】（PDF形式）

#### <http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v1.1_diff.pdf>

### サイバーセキュリティ経営ガイドラインVer 1.1付録Ｂ－２ 技術対策の例【2016年12月METI】

#### <http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_app_B-2.pdf>

## サイバーセキュリティ経営ガイドライン解説書【2016年12月IPA】

### 解説書：サイバーセキュリティ経営ガイドライン解説書（PDF：3.7MB）

#### <http://www.ipa.go.jp/files/000056148.pdf>

### 別添　：被害事例集（Excel：78.9KB）

#### <http://www.ipa.go.jp/files/000056149.xlsx>

# [政府機関向けサイバーセキュリティ対策 - CyberSec diary【新規更新中】](http://cybersec.hatenadiary.jp/entry/gov_response)

## NISC第９回会合（持ち回り開催）（平成２８年８月３１日）

### <http://www.nisc.go.jp/conference/cs/index.html>

### サイバーセキュリティ2016

#### <http://www.nisc.go.jp/active/general/pdf/kihan28.pdf>

### 政府機関の情報セキュリティ対策のための統一規範

#### <http://www.nisc.go.jp/active/general/pdf/kihan28.pdf>

### 政府機関等の情報セキュリティ対策の運用等に関する指針

#### <http://www.nisc.go.jp/active/general/pdf/shishin28.pdf>

### 政府機関の情報セキュリティ対策のための統一基準（平成28年度版）

#### <http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf>

### サイバーセキュリティ政策の評価に係る基本方針

#### <http://www.nisc.go.jp/active/kihon/pdf/cs_hyouka_houshin.pdf>

# [•サイバーセキュリティとは - CyberSec diary](http://cybersec.hatenadiary.jp/entry/what_sec)

## ■サイバーセキュリティとは

### •サイバーとは

#### ◦インターネットが形成する仮想空間（サイバースペース）

### •サイバー攻撃とは、

#### ◦コンピューターシステムやネットワークを対象に、破壊活動やデータの窃取、改ざんなどを行うこと。

#### ◦特定の組織や企業、個人を標的にする場合や、不特定多数を無差別に攻撃する場合がある。

### •サイバーセキュリティとは

#### ◦サイバー攻撃に対する防御行為。コンピューターへの不正侵入、データの改竄や破壊、情報漏洩、コンピューターウイルスの感染などがなされないよう、コンピューターやコンピューターネットワークの安全を確保すること。

### •サイバーセキュリティ基本法において、

#### ◦電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていること。

# [•情報セキュリティに関する基礎知識 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_prime_kb)

## 1.1. 情報セキュリティ対策の基本

## 1.2. 【対策】情報セキュリティ 10 大脅威（個人）

## 1.3. 【対策】情報セキュリティ 10 大脅威（組織）

## 1.4. 【対策】注目すべき脅威や懸念

## 1.5 サービス提供と情報セキュリティ対策

# [•情報セキュリティ対策の概念 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_response_concept)

## 1.1. リスクの要因

## 1.2. 情報セキュリティにおけるさまざまな対策

## 1.3. 情報セキュリティ対策の意義

## 1.4. 情報セキュリティ対策のポイント（私見）

# [•情報セキュリティポリシー、実施手順 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_policy)

## 1.1. 情報セキュリティポリシーの構成

## 1.2. 情報セキュリティポリシー（基本方針）

## 1.3. 情報セキュリティポリシー（対策基準）

## 1.4. 情報セキュリティ実施手順

## 1.5. 情報セキュリティマネジメントシステム（ISMS）構築手順

## 1.6. ISMSとPDCAサイクル

## 1.7. 脅威・対策・脆弱性・リスクの関係

## 1.8. 情報セキュリティマネジメントの規格や標準

### 1.8.1. 情報セキュリティマネジメントの実践のための規範JIS Q 27002:2006

### 1.8.2. 情報セキュリティマネジメントシステム - 要求事項JIS Q 27001:2006

## 1.9. リスクマネジメント

### 1.9.1. 情報資産の格付け

### 1.9.2. ITセキュリティマネジメントのための手法（JIS TR X 0036-3:2001）

# [•情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/it_chotatsu_sec_response)

## [「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」](http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html)

## 「政府情報システムの整備及び管理に関する標準ガイドライン実務手引書」に示された要件のうち、特にセキュリティに関連する部分を抜粋し、解説を加えたもの。

## 1.1. プロジェクトの管理

## 1.2. 業務の見直し

## 1.3. 要件定義

## 1.4. 設計・開発

## 1.5. 業務の運営と改善

## 1.6. 運用及び保守

## 1.7. システム監査の計画

# [•セキュリティインシデント対応は事業継続計画（BCP）の一つ - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_bcp)

## ■BCPとは

## ■BCPはなぜ必要か？

## ■何のためにBCPを策定するのか？

## ■セキュリティインシデント対応はBCPの１つ

# [•小規模サイトにおける情報システム担当者が持つべき知識とスキル - CyberSec diary](http://cybersec.hatenadiary.jp/entry/chusho_it_tanto_kb_skill)

## 1.1. ITパスポート試験シラバス

## 1.2. まとめ）企業の情報セキュリティ対策と人材面の対策

## 1.3. 情報処理技術者試験　情報セキュリティ人材育成の取り組み

## 1.4. 情報セキュリティマネジメント試験　シラバス

## 1.5. 情報セキュリティマネジメントタスクプロフィール

## 1.6. 情報セキュリティ人材の職種

# [•情報セキュリティマネジメントに必要な知識 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/isms_kb)

# [•サイバーセキュリティに関連したガイドライン等インデックス - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_guide_index)

## ◦公的機関、教育機関向け、個人ユーザー向け、事業者向け

## 「ここからセキュリティ！情報セキュリティ・ポータルサイト」>「対策する」>「ガイドライン等」より抜粋し補足説明。

## • 公的機関

## •教育機関向け

## •個人ユーザー向け

## •事業者向け

# [•政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/gov_std)

## ※全体的内容、規定の趣旨、対策例

# [•情報セキュリティ関連法規リスト（更新中） - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_low_list)

## 1.1. サイバーセキュリティ基本法

## 1.2. 不正アクセス禁止法

## 1.3. 個人情報保護法

## 1.4. 刑法

## 1.5. その他のセキュリティ関連法規

## 1.6. 知的財産権

## 1.7. 労働関連・取引関連法規

## 1.8. その他の法律・ガイドライン・技術者倫理

# [•サイバーセキュリティ対策公的機関・関連団体・関連機関インデックス - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_kikan_index)

## [•関連サイト [内閣サイバーセキュリティセンター]](https://www.ipa.go.jp/security/link/link.html)

## [•関連リンク：IPA 独立行政法人 情報処理推進機構](http://www.npa.go.jp/cyber/kanminboard/index.html)

## [•不正アクセス防止対策に関する官民意見集約委員会（官民ボード）](http://www.npa.go.jp/cyber/kanminboard/index.html)

## [•サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））](◦http://www.ipa.go.jp/security/J-CSIP/index.html)

## [•東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss: Tokyo Cyber Security Support network for small and medium enterprises）](http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/tcyss/index.html)

# [•サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポータルサイト - CyberSec diary](http://cybersec.hatenadiary.jp/entry/sec_total_site_list)

## [•情報セキュリティって何をするの？「ここからセキュリティ！」:情報セキュリティ・ポータルサイト（事象・対象別） 【管理者：情報処理推進機構(IPA)】](http://www.ipa.go.jp/security/kokokara/study/company.html)

### ◦「不正アクセス防止対策に関する官民意見集約委員会(官民ボード)に参加している内閣官房、警察庁、総務省及び経済産業省と民間事業者等が提供している信頼性が高く網羅的な情報群を事象・対象別に分類してナビゲートするポータルサイトです。

## [•サイトマップ[みんなでしっかりサイバーセキュリティ]【内閣官房サイバーセキュリティセンター(NISC)】](http://www.nisc.go.jp/security-site/map.html)

### ◦NISCが運営するサイバーセキュリティに関する情報のポータルです。 「スマートフォン利用者の方へ」、「家庭で」、「学校で」、「会社で」、「困ったときに」というカテゴリ別に、簡単かつ網羅的に解説されてます。

## [•国民のための情報セキュリティサイト【総務省】](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html)

### ◦インターネットと情報セキュリティの知識の習得に役だち、利用方法に応じた情報セキュリティ対策を講ずるための基本となる情報を提供しています。

## [•情報セキュリティ広場【警視庁】](http://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html)

### ◦安全な暮らしのための情報の一環で、情報セキュリティに関連する情報を体系的にわかりやすく提供しています。サイバー犯罪相談と検挙事例を通してサイバー犯罪から身を守るために必要な情報を広く都民の皆さんに提供することを目的としています。 インターネット関連企業等で構築されている「サイバー犯罪対策協議会」と連携をとって少しでもみなさんのお役に立てるページを作りました。

## [•IS702【トレンドマイクロ】](http://www.is702.jp/partner/12_t/)

## [•Security & Trust : 企業ネットワークセキュリティのためのノウハウ＆情報フォーラム 【@IT】](http://www.atmarkit.co.jp/ait/subtop/security/)

# [•中小企業の情報セキュリティ対策ガイドライン改訂版：IPA 独立行政法人 情報処理推進機構 【パブリックコメント中】](http://www.ipa.go.jp/security/keihatsu/sme/guideline/)

# [•「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec diary](http://cybersec.hatenadiary.jp/entry/tcyss_open)

# [国としての施策・基本方針・ガイドライン等の体系](#_______________________________2)

## ISMS認証基準

### JIS Q 27000：2014

#### 情報セキュリティマネジメントシステム̶用語

##### ISMSの概要、27000ファミリーの概要、ISMSファミリーで用いられる用語及び定義等についてまとめた規格

### JIS Q 27001:2014

#### ISMS適合性評価制度における認証基準

##### ISMS認証に関するガイド類

###### <https://www.isms.jipdec.or.jp/std/index.html>

### JIS Q 27002：2014

#### 情報セキュリティ管理策の実践のための規範

##### 組織の情報セキュリティリスクの環境を考慮に入れた管理策の選定、実施及び管理を含む、組織の情報セキュリティ標準及び情報セキュリティマネジメントを実施するための規範（ベストプラクティス－最良の慣行）をまとめた規格

### 【参考】

#### 地方公共団体と情報セキュリティ（2016年3月8日JIPDEC）

##### <https://www.isms.jipdec.or.jp/doc/JIP-ISMS119-20.pdf>

##### ISMSの規格改正へ対応するとともに、「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」等の更新状況を確認したもの

## 「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（平成28年度版）」（2016年8月31日サイバーセキュリティ戦略本部決定）

### <http://www.nisc.go.jp/active/general/kijun28.html>

## [企業経営のためのサイバーセキュリティの考え方の策定について【NISC】](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

### <http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf>

### [サイバーセキュリティ戦略本部](http://www.nisc.go.jp/conference/cs/index.html)

#### <http://www.nisc.go.jp/conference/cs/index.html>

### 経営層に期待される“認識”や経営戦略を企画する人材層に向けた実装のためのツールを示す

### 基本方針

#### ーサイバーセキュリティは、より積極的な経営への「投資」へー

#### サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

### I.基本的考え方

#### 二つの基本的認識

##### ＜①挑戦＞

###### 新しい製品やサービスを創造するための戦略の一環として考えていく

##### ＜②責任＞

###### サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与する

#### 三つの留意事項

##### ＜①情報発信による社会的評価の向上＞

###### • 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。

###### • そのような取組に係る姿勢や方針を情報発信することが重要。

##### ＜②リスクの一項目としてのサイバーセキュリティ＞

###### • 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。

###### • 経営層のリーダーシップが必要。

##### ＜③サプライチェーン全体でのサイバーセキュリティの確保＞

###### • サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流出するおそれあり。

###### • 一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

### II.企業の視点別の取組

#### ITの利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある

#### ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に競争力強化に活用しようとしている企業

##### （積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）

##### 【経営者に期待される認識】

###### • 積極的なITの利活用を推進する中で、製品やサービスの「セキュリティ品質」を一層高め、自社のブランド価値の向上につなげるべく、システムの基盤におけるセキュリティの向上、情報・データの保護、製品等の安全品質向上に取り組む。

###### • 様々な関係者との協働が重要であるため、情報提供に主体的に取り組む。

###### • 決して現存する標準や取り組みなどに満足することなく、実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、変革していく存在となることが期待される。

##### 【実装に向けたツール】

###### • IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）

###### • 自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

#### IT・セキュリティをビジネスの基盤として捉えている企業

##### （IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略に組み込むところまでは位置づけていない企業）

##### 【経営者に期待される認識】

###### • 経営者のリーダーシップによって、社会的責任としてのサイバーセキュリティ対策に取り組む。

###### • サプライチェーンやビジネスパートナー、委託先を含めた対策を行う。

###### • 平時・緊急時のいずれにおいても、情報開示などの適切なコミュニケーションを行う。

##### 【実装に向けたツール】

###### • サイバーセキュリティ経営ガイドライン

###### • 企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用

###### • サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

#### 自らセキュリティ対策を行う上で、事業上のリソースの制約が大きい企業

##### （主に中小企業等でセキュリティの専門組織を保持することが困難な企業）

##### 【経営者に期待される認識】

###### • サプライチェーンを通じて中小企業等の役割はますます重要となる中、消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、取り組む。

###### • 外部の能力や知見を活用しつつ、効率的に進める方策を検討する。

##### 【実装に向けたツール】

###### • 効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）

###### • サイバーセキュリティに関する相談窓口やセミナー、地域の相談員等の活用



## 「政府情報システムの整備及び管理に関する標準ガイドライン」(2015年3月19日更新、2014年12月3日各府省CIO連絡会議決定）および「実務手引書」

### <http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html>

### 世界最先端IT国家創造宣言(2013年6月14日閣議決定。2014年6月24日変更)に基づき、政府におけるITガバナンス強化のため、情報システム調達やプロジェクト管理に関する共通ルールとして策定

#### [世界最先端IT国家創造宣言(2013年6月14日閣議決定。2014年6月24日変更)](http://www.soumu.go.jp/main_content/000352690.pdf)