

☐ Sec01-06 サイバーセキュリティ専門員による情報収集・整理・蓄積・提供

■ 【2018年1月24日加筆】

☐ 中小企業におけるセキュリティ対策に必要な知識とスキル

☐ 中小企業の活性化は、国家的課題

- 日本の企業数の99.7%、従業員数で7割を占めると言われる中小企業。中小企業が活性化しない限り、日本経済の復興、地域創生はあり得ない。

☐ 中小企業の現状と課題

☐ 人材不足

- 数
- 質

☐ 資金不足

☐ 効率化資金不足

- IT化資金
- セキュリティ対策資金
- 新ビジネス展開資金不足

☐ 中小企業における変革の必要性

☐ IT化、デジタル化社会の急速

- 現状のままでは、ビジネスは衰退する
- ITを活用しなければサイバーセキュリティ対策は必要ない
- ITを活用しなければ、競争力を失い、事業は現状維持どころか、継続も危ぶまれる

☐ 経営者が、IT社会、デジタル社会での対応の意識を持っている企業

☐ 人材不足の解消のためには

- IT活用が必須
- IT人材が必要

☐ IT活用のためには、

- セキュリティ対策が必須
- セキュリティ人材が必要

☐ 費用対効果の高いIT活用のためには

- IT化と同時にセキュリティ対策を行うことが経済的

☐ 経営者が、対応の意識を持っていない企業

- 経営者の意識改革が必要
- 自社が被害者になる
- 他社への加害者になる

■ 事業継続ができなくなる

□ 例えば

- インターネット接続していないから大丈夫？わが社に限って（他人事だと思っている）
- Windows、ウイルスによる脆弱性をそのまま放置
 - USB等を接続するとウイルス感染の恐れ
 - そのUSB等を媒介して、他者のPCにウイルス感染の恐れ
 - 自社の重要情報が破壊される恐れ
 - 他社に感染させると、
 - 他社の重要情報が破壊される恐れ
 - 他社の営業機密情報の漏えいの恐れ
 - 社会的信用の喪失
 - ビジネスの継続が困難になる

□ 収集

□ 収集すべき情報






- 国及び関係機関が公開しているガイドブック類の内容概要
- 関係機関がウェブ公開しているセキュリティ関連情報の所在場所と概要
- 関係機関が発信した緊急情報

□ 収集元




□ 事前調査

□ IT・セキュリティ関連サイト内ページ、ドキュメント






















□ 一般ユーザ向け


















- インターネットを安全に利用するための情報セキュリティ対策9か条【NISC・IPA】 
- ① ネットワークビギナーのための情報セキュリティハンドブック（小冊子）【2016年02月02日NISC】⇒【2016年12月02日NISC】 
- マンガで学ぶサイバーセキュリティ【NISC】【初心者向け】 
- 基礎知識 | 国民のための情報セキュリティサイト【総務省】 
- 一般利用者の対策 | 国民のための情報セキュリティサイト【総務省】 


















□ 企業向け（特に中小企業）


- ① 中小企業の情報セキュリティ対策ガイドライン（第2.1版）【2017年5月IPA】 
- 中小企業における組織的な情報セキュリティ対策ガイドラインチェック項目【2012年9月3日IPA】 
- 中小企業における組織的な情報セキュリティ対策ガイドライン事例集【2012年9月3日IPA】 







Expand - Collapse


- SECURITY ACTION【2017年4月IPA】 
- 中小企業における情報セキュリティの普及促進に関する共同宣言 
- 企業向け（全ての企業・組織）
 - 情報セキュリティ白書2016【2016年7月IPA】 
 - 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【2015年8月21日IPA】 
 - 組織における内部不正防止ガイドライン（日本語版） 第4版ガイドライン【2017年1月31日IPA】 
 - スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書【2015年 5月21日NISC】 
 - 情報セキュリティ読本 四訂版- IT時代の危機管理入門 -【2014年11月4日IPA】 
 - 情報セキュリティ 10 大脅威（組織）【2017年3月IPA】 
 - 企業・組織の対策 | 国民のための情報セキュリティサイト【総務省】 
 - @police－被害事例と対処法【警察庁】 
 - 情報セキュリティポリシーサンプル改版（1.0版）【2016年3月29日JNSA】 
 - すぐ役立つ！法人で行うべきインシデント初動対応～「不審な通信」その時どうする～【トレンドマイクロ】
 - ②【てびき】情報管理も企業力～秘密情報の保護と活用～【2016年12月5日METI】 
 - 「企業における営業秘密管理に関する実態調査」報告書について【2017年3月17日IPA】 
 - 改正個人情報保護法（2017年5月改正施行）対応 
 - コンピュータセキュリティインシデント対応ガイド（NIST SP 800-61）【2008年3月NIST】 
- 企業向け（零細企業を除く）
 - 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8日METI】 
 - ① サイバーセキュリティ経営ガイドライン解説書Ver.1.0【2016年12月IPA】
 - ② 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【2016年8月2日NISC】 
 - 米国の「20の重要なセキュリティ対策」及びオーストラリアの「35の標的型サイバー侵入に対する軽減戦略」
- 重要インフラ・政府機関向け（独法を含む）
 - サイバーセキュリティ2016【2016年8月31日NISC】 
 - 政府機関の情報セキュリティ対策のための統一規範 
 - 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 
 - 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） 

- 政府機関向け「アマゾン ウェブ サービス」対応セキュリティ [ス](#) 
- ① 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【2016年8月2日NISC】 [ス](#) 
- 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定について【2015年5月NISC】 [ス](#) 
- 知的財産関連
 - 「第四次産業革命を視野に入れた知財システムの在り方に関する検討会」の報告書の中小企業部分抜粋 [ス](#) 
- 次世代IT技術及び市場動向
 - IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】 [ス](#) 
 - 安全なIoTシステムの創出【2016年3月1日NISC】 [ス](#) 
 - コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】 [ス](#) 
 - IoT早期導入者のためのセキュリティガイダンス【2016年2月24日CSA】 [ス](#) 
 - クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】 [ス](#) 
 - クラウドサービス提供における情報セキュリティ対策ガイドライン【2014年4月総務省】 [ス](#) 
- クラウドセキュリティ関連ISO規格
 - ■ ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（スライド）【JIPDEC】 [ス](#) 
 - ■ ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】 [ス](#) 
 - ■ ISO/IEC27017:2015に基づくクラウドセキュリティの構築のポイント（スライド）【JIPDEC】 [ス](#) 
 - 教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック【総務省】 [ス](#) 
 - 教育 I C Tの新しいスタイルクラウド導入ガイドブック2015【総務省】 [ス](#) 
- システム化及びサイバーセキュリティ管理規約等
 - 人材育成・人材確保
 - ■ iコンピテンシ・ディクショナリ【IPA】 [ス](#) 
 - ■ ITのスキル指標を活用した情報セキュリティ人材育成ガイド【2015年5月IPA】 [ス](#) 
 - 情報処理安全確保支援士試験チェックシート
 - ISMS関連
 - ■ ISMSユーザーズガイド-JISQ27001:2014(ISO/IEC27001:2013)対応【JIPDEC】

- ■ ISMSユーザズガイド-JISQ27001:2014(ISO/IEC 27001) 応-リスクマネジメント編【JIPDEC】
- 情報セキュリティマネジメントシステム(ISMS) 適合性評価制度
- 情報セキュリティマネジメント (ISMS) に準拠した対策【ISO/IEC27001:2013 (管理項目35, 管理策114)】
- ▢ 施策・政策・統計
 - [サイバーセキュリティ関連施策に関する平成29年度予算重点化方針](#) 
 - [サイバーセキュリティ政策の評価に係る基本方針](#) 
- ▢ IT・セキュリティ関連書籍
 - ▢ 情報処理技術者試験シラバス、テキスト、過去問題集
 - ITストラテジスト試験
 - 応用情報技術者試験
 - 情報処理安全確保支援士試験
 - 情報セキュリティマネジメント試験
 - ITパスポート試験
 - CISSP(Certified Information Systems Security Professional)
 - 公認情報セキュリティマネージャー (CISM)
- ▢ 日々動向
 - ▢ Yammer (TCYSSメンバー限り)
 - ▢ [中小企業向け最新セキュリティ情報](#) 
 - 各機関が公開もしくは公開準備をしている情報
 - ▢ Twitter
 - マルウェア情報局 @MalwareInfo_JP
 - 内閣サイバー(注意・警戒情報)  認証済みアカウント  @nisc_forecast
 - IPA (情報処理推進機構) @IPAjp
 - JVN 脆弱性レポート @jvnjp
 - IPA (ICATalerts)  認証済みアカウント  @ICATalerts
 - マイクロソフト セキュリティチーム  認証済みアカウント  @JSECTEAM
 - マカフィー株式会社 @McAfee_JP
 - カスペルスキー 公式  認証済みアカウント  @kaspersky_japan
 - ノートン 公式 ツイッター  認証済みアカウント  @NortonJapan
 - トレンドマイクロ  認証済みアカウント  @trendmicro_jp
 - エフセキュアブログ @FSECUREBLOG
 - 情報セキュリティのラック @lac_security
 - JPCERTコーディネーションセンター  認証済みアカウント  @jpcert
 - ▢ ニュースサイト、ブログサイト

- ▢ Googleニュース
 - セキュリティ, 脆弱性, 脅威
 - @IT Security&Trustフォーラム
 - Security NEXT
 - セキュリティホール memo
 - 高木浩光@自宅の日記
 - 統合版 JPCERT/CC RSS
 - 日本のセキュリティチーム
 - . . .
- ▢ ブックマーク情報（はてなブックマーク等）
 - タグ：セキュリティ
- ▢ 収集担当
 - ▢ 「セキュリティリサーチャー」
 - 東京都、警視庁の担当者
 - TCYSSメンバー機関担当者
- ▢ 収集方法
 - ▢ （TCYSSメンバー限り）
 - 「中小企業向け最新セキュリティ情報」グループで情報交換
 - ▢ Twitter
 - 信頼できる情報を提供しているTwitterアカウントをリスト化
 - リストをブログパーツ化
 - ▢ ニュースサイト
 - ▢ Googleニュースのニュースキーワードで選択
 - セキュリティ, 脆弱性, 脅威
 - Feeldy等のRSSリーダでのサイト一括閲覧
- ▢ 整理して知識化（ノウハウ化）
 - ▢ 整理担当
 - 東京都、警視庁の担当者
 - TCYSSメンバー機関担当者
 - ▢ 近い将来（2～3年後）
 - 収集情報をビッグデータ化しAIサービスにより、整理・知識化
 - 相談業務は、バックオフィスでAIサービスを利用
 - さらに、相談者が直接利用できるようなAIサービスをウェブで公開
- ▢ 知識化すべき情報
 - IT・セキュリティ関連サイト内ページ、ドキュメントの要約 
 - IT・セキュリティ関連書籍の要約

- 日々動向情報から重要度、緊急度の高い情報を選択 
- 知識化方法
 - YammerでのTCYSSメンバーによる意見交換で
 - 東京都、警視庁の担当者の日常業務で
- 情報発信
 - Webページで発信
 - 意識すること
 - 日々更新されなければ、固定ユーザは付かない
 - 担当組織、担当者が変わっても維持できること
 - システム運用
 - サーバ管理者を不要とする
 - コンテンツ管理
 - 日々の相談対応のための情報収集の一環で
 - 「走りながら考える」（TCYSS発足時の課長発言）
 - 1年以上立ち止まった状態に見える
 - 東京都の実施姿勢
 - 都政改革を進める視点
 - 都民ファースト 
 - 情報公開
 - 積極的にかつタイムリーに情報公開 
 - 税金の有効活用（ワイズ・スペンディング） 
 - 東京都職員のミッション（HPより）
 - 都民ファーストの視点を常に持つ
 - 視野を広げ、常にチャレンジする
 - ライフ・ワーク・バランスを実践する
 - 公務員倫理に沿って
 - 少ない費用で効率的に 
 - 迅速性を重視
 - 手順を踏むことや書類を整えることを重視させない 
 - 国民目線で常に創意工夫
 - 少ない費用でより効率的に
 - ハードウェア、ソフトウェア、ネットワーク、セキュリティの運用はプロバイダサービスに任せる
 - レンタルWebサーバ

- Blog等のサイト
- TCYSSメンバー企業であるMicrosoftのOffice365
- 迅速性を重視
 - 暫定対応
 - まずは、Blog等でプロトタイプ的に
 - 恒久的対応
 - レンタルWebサーバにするか、Blogのまま続けるか検討
 - 予算は、デザイン料のみ
- TCYSSとしての発信
 - TCYSS参加機関の相互協定に基づいて
 - 東京都のウェブページである必要がないのではないか
 - .tokyoドメイン等を取得（t c y s s .tokyoとか）
 - 相談員としてのモチベーションの向上
- 発信する情報
 - 相談業務の一環で日々収集しているホットな情報の中から、中小企業向けの情報を引用しコメント付けしてアップ 
 - 相談業務の一環で、整理して知識化したものを定期的に掲載
- Twitter等
 - 日々アップしたページをツイート
 - 関係機関が発信した情報のうち、重要度の高いものをリツイート
- 進めるにあたって
 - TCYSS相互協力協定に基づく
 - まずは参加者や期間を限定した「規制のサンドボックス」制度による
 - 規制改革、行政手続き簡素化に繋げることも留意