

## CyberSec's Diary

CyberSec's Diary.....	1
1. 中小企業サイバーセキュリティ対策関連の備忘録.....	15
1.1. 緊急対応時のピックアップ情報.....	15
1.2. 情報セキュリティが心配になったら - CyberSec's diary .....	15
1.3. 相談対応手引き関連.....	15
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's diary   16	
1.3.2. ●情報セキュリティ緊急対応ガイド【汎用】 - CyberSec's diary.....	16
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's diary   16	
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's diary   16	
1.4. 事例（FAQ候補） .....	16
1.4.1. ●セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec's diary ...	16
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's diary..	16
1.5. 情報化推進のためのセキュリティ対策.....	16
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 .....	17
1.6. 中小企業向けの情報セキュリティ対策関連.....	17
1.6.1. ●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】 .....	17
1.6.2. 中小企業に特化した情報セキュリティ対策の相談対応【私見】 - CyberSec's diary.....	18
1.6.3. ●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's diary.....	18
1.6.4. ●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's diary   18	
1.6.5. ●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's diary.....	18
1.7. 家庭個人向け.....	18
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's diary【更新中】 .....	19
1.8. 重要インフラ関連.....	19
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's diary【更新中】 .....	19

1.9.	情報セキュリティマネジメント関連.....	19
1.9.1.	•サイバーセキュリティとは - CyberSec's diary.....	19
1.9.2.	•情報セキュリティに関する基礎知識 - CyberSec's diary.....	19
1.9.3.	•情報セキュリティ対策の概念 - CyberSec's diary.....	19
1.9.4.	•情報セキュリティポリシー、実施手順 - CyberSec's diary.....	19
1.9.5.	•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's diary.....	19
1.9.6.	•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's diary.....	20
1.10.	人材育成・人材確保.....	20
1.10.1.	•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's diary.....	20
1.10.2.	•情報セキュリティマネジメントに必要な知識 - CyberSec's diary ..	20
1.11.	関連基準、法規、対策機関等.....	20
1.11.1.	•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's diary.....	20
1.11.2.	•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's diary.....	20
1.11.3.	•情報セキュリティ関連法規リスト（更新中） - CyberSec's diary ..	21
1.11.4.	•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's diary.....	21
1.12.	セキュリティ関連情報提供サイト一覧.....	21
1.12.1.	•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's diary.....	21
1.13.	ニュース.....	21
1.13.1.	•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】.....	21
1.13.2.	•「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec's diary.....	21
2.	緊急対応時のピックアップ情報.....	22
3.	情報セキュリティが心配になったら - CyberSec's diary.....	22
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.....	22

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)	22
3.2.	【緊急】セキュリティ侵害の可能性はあるが、どこに問い合わせていいかわからない？	23
3.2.1.	•「中小企業サイバーセキュリティ対策相談窓口」へ	23
3.3.	【緊急】情報の漏えい・改ざんが起きている？	23
3.3.1.	•犯罪の可能性がある場合は、警視庁へ	23
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？	24
3.4.1.	•ウイルス感染、不正アクセスの可能性	24
3.5.	【緊急】実被害にあった場合	25
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。	25
3.5.2.	•ウイルス・不正アクセス届出	25
3.5.3.	•インシデント報告・届出	26
3.5.4.	•サイバー犯罪届出（全国）	26
3.6.	【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？	26
3.6.1.	•消費者ホットライン	27
3.6.2.	•暮らしにかかわる東京都の情報サイト	27
3.7.	【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	27
3.7.1.	•情報セキュリティ対策の基本を知る	27
3.8.	【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？	28
3.8.1.	•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	28
3.8.2.	•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	29
3.8.3.	•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)	29
3.9.	参考情報	29
3.9.1.	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を解説します	30
3.9.2.	中小企業向けサイバーセキュリティ関連ニュース	30

3.10.	他のページへのリンク .....	31
3.10.1.	中小企業サイバーセキュリティ対策関連の備忘録 - CyberSec's diary 31	
4.	•サイバーセキュリティ相談・届出先クイックリスト - CyberSec's diary .....	31
4.1.	凍結中 .....	31
5.	•情報セキュリティ緊急対応ガイド【汎用】 - CyberSec's diary .....	31
5.1.	■緊急対応（自然災害, 大火災, 感染症, テロ,,,） .....	32
5.1.1.	事象の検知、報告受付(Detect) .....	32
5.1.2.	事実確認、対応の判断 被害の局所化(拡大防止)(Triage) .....	32
5.1.3.	緊急連絡 .....	32
5.1.4.	原状保全 .....	32
5.1.5.	原因調査 .....	33
5.1.6.	早期復旧・事業継続 (Respond) .....	33
5.1.7.	恒久的対策（再発防止策） .....	33
5.1.8.	通常運用 .....	34
5.2.	■情報セキュリティ対策の必要性 .....	35
5.2.1.	<ul style="list-style-type: none"> <li>•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。 .....</li> </ul>	35
5.2.2.	<ul style="list-style-type: none"> <li>•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 .....</li> </ul>	35
5.2.3.	•情報セキュリティ対策は、事業継続計画の一つ .....	35
5.2.4.	<ul style="list-style-type: none"> <li>•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 35</li> </ul>	
5.2.5.	<ul style="list-style-type: none"> <li>•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 .....</li> </ul>	35
5.3.	■情報セキュリティ対策の基本 .....	36
5.3.1.	情報セキュリティ侵害とは .....	36
5.3.2.	脅威・手口を知る（10大脅威2016簡易説明資料（組織編）） .....	36
5.3.3.	情報資産の認識 .....	38

5.3.4.	リスク分析 .....	38
5.3.5.	対策はリスクの高いものを優先する .....	38
5.3.6.	恒久的対策 .....	39
5.3.7.	定期的な監査 .....	42
5.4.	■参考資料 .....	42
6.	●相談対応の手引きレファレンスリスト【相談員用】 - CyberSec's diary .....	42
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 .....	42
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's diary .....	42
6.2.	■事例等の紹介 .....	42
6.2.1.	●セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec's diary .....	43
6.3.	■対策まとめ資料 .....	43
6.3.1.	●情報セキュリティ対策とは .....	43
6.3.2.	●中小企業向け対策 .....	43
6.3.3.	●システム調達におけるセキュリティ要件定義 .....	44
6.3.4.	—————相談対応の手引き用【更新中】————— .....	44
7.	●サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec's diary .....	44
7.1.	●サイバーセキュリティ対策相談対応の手引き（メモ） .....	44
7.1.1.	展開した文書 .....	45
8.	●セキュリティ侵害事例紹介サイト（FAQ候補） - CyberSec's diary .....	45
8.1.	各種Webから抜粋したページ .....	45
8.2.	○相談窓口対応事例（FAQ候補） - CyberSec's diary .....	45
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's diary .....	45
9.1.	「ここからセキュリティ」を展開したページ .....	45
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】 .....	45
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 .....	46
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 .....	46
10.1.2.	セキュリティ侵害の実態 .....	50
10.1.3.	情報セキュリティ対策の必要性の認識が必要 .....	51
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 .....	54
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 .....	54
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's diary ㊦【作成中】 .....	55

11.1.	【作成中】 .....	55
11.2.	■活用戦略.....	55
11.3.	■活用技術.....	55
11.4.	●クラウドコンピューティング.....	55
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's diary.....	55
12.1.	対象範囲と役割分担.....	55
12.2.	中小企業の現状.....	55
12.2.1.	●組織の意識と対策.....	56
12.2.2.	●実態調査.....	57
12.3.	中小企業への支援.....	58
12.3.1.	●普及啓発.....	58
12.3.2.	●対策の概要.....	60
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's diary.....	63
13.1.	■緊急相談対応.....	63
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's diary 63	
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).....	64
13.1.3.	●情報セキュリティに関する基礎知識 - CyberSec's diary.....	64
13.1.4.	●情報セキュリティ緊急対応ガイド - CyberSec's diary.....	65
13.2.	■中小企業経営者向け情報.....	65
13.2.1.	●情報セキュリティ対策9カ条【NISC,IPA】(pdf形式).....	66
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】.....	66
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).....	66
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ー一覧【IPA】..	67
13.2.5.	●その他の各種情報へのリンク.....	67
13.3.	■家庭・個人向け情報.....	67
13.3.1.	●【準備中】.....	68
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.....	68
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's diary（準備中）.....	68

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.....	68
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's diary.....	68
13.6.	■人材育成・人材確保.....	68
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's diary.....	68
13.6.2.	•情報セキュリティマネジメント -- XMind Online Library .....	68
13.7.	■参考情報.....	68
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's diary.....	69
13.7.2.	•情報セキュリティ関連法規リスト（更新中） - CyberSec's diary ..	69
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's diary.....	69
13.8.	■関連ニュース.....	69
13.9.	————— 相談対応の手引き用 ————— .....	69
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 69	
13.9.2.	■事例等の紹介 .....	70
13.9.3.	■対策まとめ資料 .....	70
13.10.	————— 相談対応の手引き用【更新中】 ————— .....	71
13.10.1.	【更新中】 .....	72
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's diary.....	72
14.1.	■対象範囲と役割分担.....	72
14.2.	■中小企業の現状.....	72
14.3.	■中小企業への支援.....	72
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's diary.....	72
15.1.	■サイバーセキュリティ対策の必要性.....	72
15.1.1.	•情報セキュリティの脅威.....	73
15.1.2.	•守るべき情報資産の認識.....	73
15.1.3.	•最低限の対策.....	73
15.2.	■理解度確認.....	73
15.3.	■対策のしおり .....	73

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 .....	73
15.4.1.	※主なサイトへのリンク .....	73
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 .....	73
15.5.1.	※主なサイトへのリンク .....	73
16.	・家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec's diary【更新中】 .....	74
16.1.	更新中 .....	74
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's diary【更新中】 .....	74
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）【LEVEL1】【詳細】【冊子】 .....	74
17.1.1.	<a href="http://www.nisc.go.jp/conference/cs/dai07/pdf/07shiryou02.pdf">http://www.nisc.go.jp/conference/cs/dai07/pdf/07shiryou02.pdf</a> .....	74
17.2.	・【●】サイバーセキュリティ経営ガイドライン(経済産業省)【LEVEL1】【詳細】【冊子】 .....	74
17.2.1.	<a href="http://www.meti.go.jp/press/2015/12/20151228002/20151228002.htm">http://www.meti.go.jp/press/2015/12/20151228002/20151228002.htm</a> .....	74
17.2.2.	<a href="http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf">http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf</a> .....	75
17.3.	更新中 .....	75
18.	・サイバーセキュリティとは - CyberSec's diary .....	75
18.1.	■サイバーセキュリティとは .....	75
18.1.1.	・サイバーとは .....	75
18.1.2.	・サイバー攻撃とは、 .....	75
18.1.3.	・サイバーセキュリティとは .....	76
18.1.4.	・サイバーセキュリティ基本法において、 .....	76
19.	・情報セキュリティに関する基礎知識 - CyberSec's diary .....	77
19.1.	1.1. 情報セキュリティ対策の基本 .....	77
19.2.	1.2. 【対策】情報セキュリティ 10 大脅威（個人） .....	77
19.3.	1.3. 【対策】情報セキュリティ 10 大脅威（組織） .....	77
19.4.	1.4. 【対策】注目すべき脅威や懸念 .....	77
19.5.	1.5 サービス提供と情報セキュリティ対策 .....	77
20.	・情報セキュリティ対策の概念 - CyberSec's diary .....	77



20.1.	1.1.	リスクの要因 .....	77
20.2.	1.2.	情報セキュリティにおけるさまざまな対策 .....	77
20.3.	1.3.	情報セキュリティ対策の意義 .....	77
20.4.	1.4.	情報セキュリティ対策のポイント（私見） .....	77
21.		●情報セキュリティポリシー、実施手順 - CyberSec's diary .....	77
21.1.	1.1.	情報セキュリティポリシーの構成 .....	78
21.2.	1.2.	情報セキュリティポリシー（基本方針） .....	78
21.3.	1.3.	情報セキュリティポリシー（対策基準） .....	78
21.4.	1.4.	情報セキュリティ実施手順 .....	78
21.5.	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 .....	78
21.6.	1.6.	ISMSとPDCAサイクル .....	78
21.7.	1.7.	脅威・対策・脆弱性・リスクの関係 .....	78
21.8.	1.8.	情報セキュリティマネジメントの規格や標準 .....	78
21.8.1.	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 .....	78
21.8.2.	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 .....	78
21.9.	1.9.	リスクマネジメント .....	78
21.9.1.	1.9.1.	情報資産の格付け .....	79
21.9.2.	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） .....	79
22.			
		●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's diary .....	79
22.1.			
		「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」 .....	79
22.2.			
		「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。 .....	79
22.3.	1.1.	プロジェクトの管理 .....	79
22.4.	1.2.	業務の見直し .....	79
22.5.	1.3.	要件定義 .....	79
22.6.	1.4.	設計・開発 .....	79
22.7.	1.5.	業務の運営と改善 .....	80
22.8.	1.6.	運用及び保守 .....	80
22.9.	1.7.	システム監査の計画 .....	80

23.	●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's diary	80
23.1.	■BCPとは	80
23.2.	■BCPはなぜ必要か？	80
23.3.	■何のためにBCPを策定するのか？	80
23.4.	■セキュリティインシデント対応はBCPの1つ	80
24.	●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's diary	80
24.1.	1.1. ITパスポート試験シラバス	80
24.2.	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	80
24.3.	1.3. 情報処理技術者試験②情報セキュリティ人材育成の取り組み	80
24.4.	1.4. 情報セキュリティマネジメント試験②シラバス	80
24.5.	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	81
24.6.	1.6. 情報セキュリティ人材の職種	81
25.	●情報セキュリティマネジメントに必要な知識 - CyberSec's diary	81
26.	●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's diary	81
26.1.	○公的機関、教育機関向け、個人ユーザー向け、事業者向け	81
26.2.	「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。	81
26.3.	●公的機関	81
26.4.	●教育機関向け	81
26.5.	●個人ユーザー向け	81
26.6.	●事業者向け	81
27.	●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's diary	81
27.1.	※全体的内容、規定の趣旨、対策例	82
28.	●情報セキュリティ関連法規リスト（更新中） - CyberSec's diary	82
28.1.	1.1. サイバーセキュリティ基本法	82
28.2.	1.2. 不正アクセス禁止法	82
28.3.	1.3. 個人情報保護法	82
28.4.	1.4. 刑法	82
28.5.	1.5. その他のセキュリティ関連法規	82
28.6.	1.6. 知的財産権	82
28.7.	1.7. 労働関連・取引関連法規	82
28.8.	1.8. その他の法律・ガイドライン・技術者倫理	82

29.	●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's diary.....	82
29.1.	●関連サイト [内閣サイバーセキュリティセンター].....	82
29.2.	●関連リンク：IPA 独立行政法人 情報処理推進機構.....	82
29.3.	●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） 83	
29.4.	●サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））.....	83
29.5.	●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）.....	83
30.	●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's diary.....	83
30.1.	●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)】.....	83
30.1.1.	○「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。.....	83
30.2.	●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)】.....	83
30.2.1.	○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。 84	
30.3.	●国民のための情報セキュリティサイト【総務省】.....	84
30.3.1.	○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。.....	84
30.4.	●情報セキュリティ広場【警視庁】.....	84
30.4.1.	○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。	84
30.5. •IS702【トレンドマイクロ】	85
30.6. •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】	85
31. •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】	85
32. •「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec's diary	85
33. 国としての施策・基本方針・ガイドライン等の体系	85
33.1. ISMS認証基準	85
33.1.1. JIS Q 27000 : 2014	86
33.1.2. JIS Q 27001:2014	86
33.1.3. JIS Q 27002 : 2014	87
33.1.4. 【参考】	87
33.2.	
「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）	88
33.2.1. <a href="http://www.nisc.go.jp/active/general/kijun28.html">http://www.nisc.go.jp/active/general/kijun28.html</a>	88
33.3.	
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】	88
33.3.1. <a href="http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf">http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf</a>	88
33.3.2. サイバーセキュリティ戦略本部	88
33.3.3.	
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	89
33.3.4. 基本方針	89
33.3.5. I.基本的考え方	89
33.3.6. II.企業の視点別の取組	92
33.4.	
「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」	96
33.4.1. <a href="http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html">http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html</a>	96
33.4.2.	
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 .....	96
---	----

## CyberSec's Diary

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  
情報セキュリティが心配になったら - CyberSec's diary

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

情報セキュリティ緊急対応ガイド【汎用】 - CyberSec's diary

相談対応の手引きレファレンスリスト【相談員用】 - CyberSec's diary

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

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

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's diary

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】

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's diary 【作成中】

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's diary

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's 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's diary

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's diary

家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec's diary【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's diary【更新中】

サイバーセキュリティとは - CyberSec's diary

情報セキュリティに関する基礎知識 - CyberSec's diary

情報セキュリティ対策の概念 - CyberSec's diary

情報セキュリティポリシー、実施手順 - CyberSec's diary

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's 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's diary

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's diary

情報セキュリティマネジメントに必要な知識 - CyberSec's diary

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's 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's diary

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

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's diary

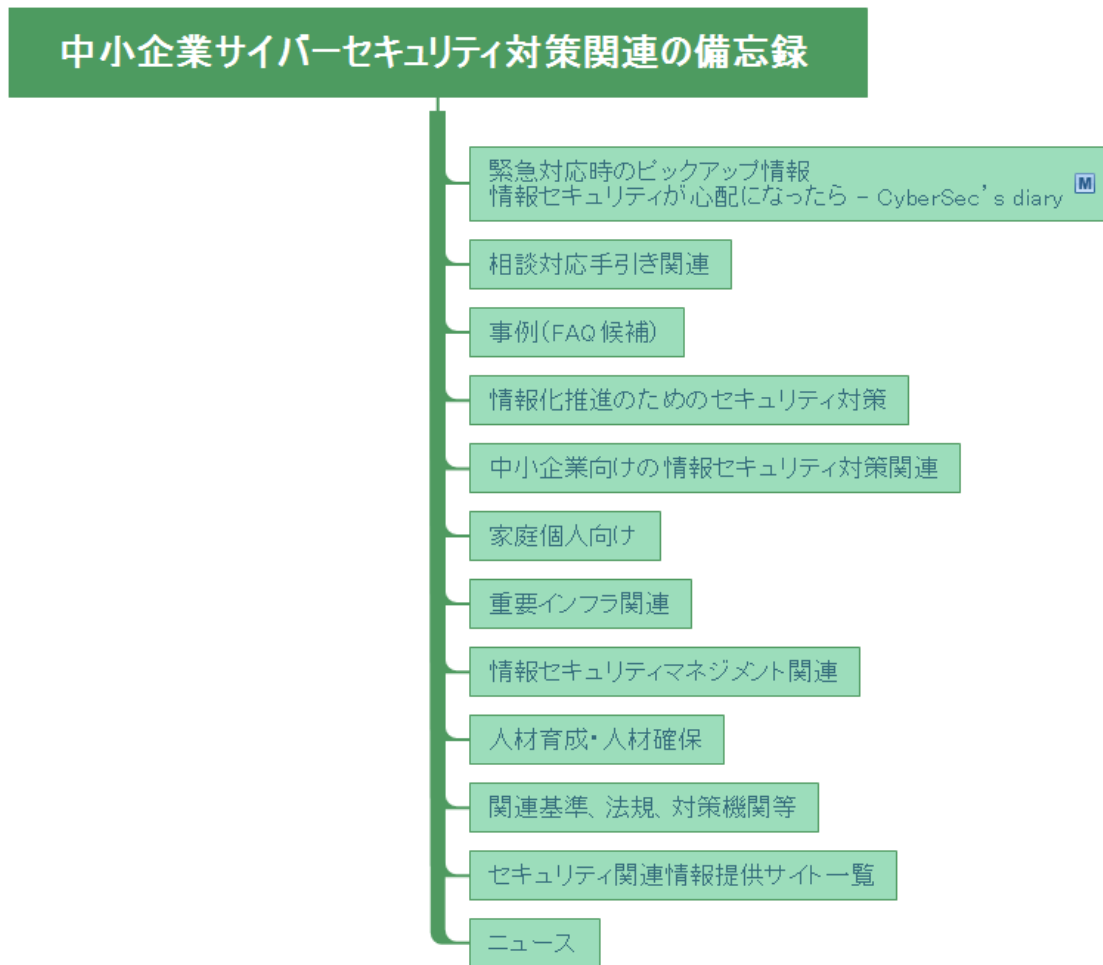
サイバーセキュリティ全般の体系的・網羅的な情報を提供しているポ  
ータルサイト - CyberSec's diary

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】

「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec's diary

国としての施策・基本方針・ガイドライン等の体系

## 1. 中小企業サイバーセキュリティ対策関連の備忘録







### 1.1. [緊急対応時のピックアップ情報](#)

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

### 1.3. 相談対応手引き関連

## 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's diary 
- ・情報セキュリティ緊急対応ガイド【汎用】 - CyberSec's diary 
- ・相談対応の手引きレファレンスリスト【相談員用】 - CyberSec's diary 
- ・サイバーセキュリティ対策相談対応の手引き（メモ） - CyberSec's diary 

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's diary](#)



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

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's diary](#)

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's diary](#)

## 1.4. 事例（FAQ候補）

### 事例（FAQ候補）

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

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

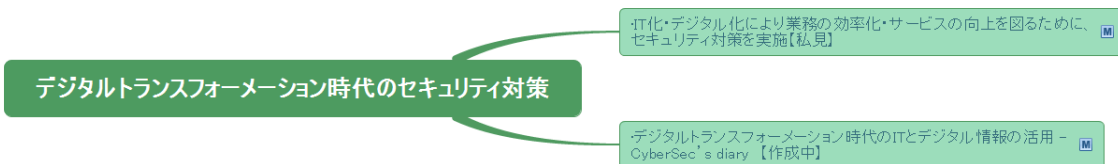
1.4.2. [・ここからセキュリティ！  
情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 - CyberSec's diary](#)

## 1.5. 情報化推進のためのセキュリティ対策





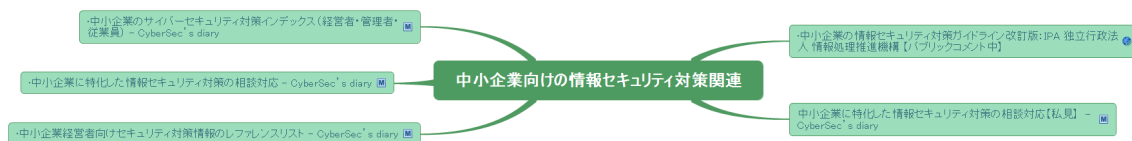
### 1.5.1. デジタルトランスフォーメーション時代のセキュリティ対策



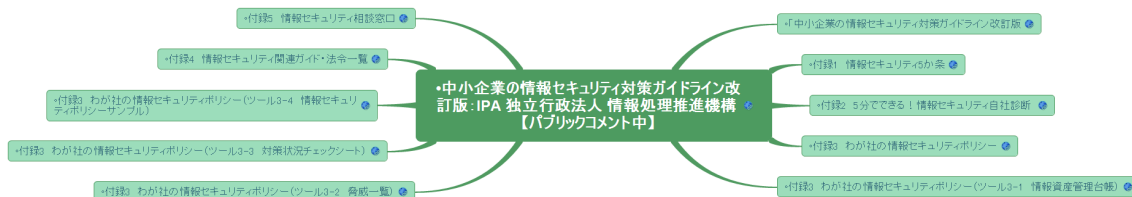
1.5.1.1. ●IT化・デジタル化により業務の効率化・サービスの向上を図るために、セキュリティ対策を実施【私見】

1.5.1.2. ●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's diary【作成中】

### 1.6. 中小企業向けの情報セキュリティ対策関連



1.6.1. ●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】



1.6.1.1. 。「中小企業の情報セキュリティ対策ガイドライン改訂版

1.6.1.2. 。付録10情報セキュリティ5か条

1.6.1.3. [◦付録2回5分でできる！情報セキュリティ自社診断](#)

1.6.1.4. [◦付録3回わが社の情報セキュリティポリシー](#)

1.6.1.5. [◦付録3回わが社の情報セキュリティポリシー（ツール3-1回  
情報資産管理台帳）](#)

1.6.1.6. [◦付録3回わが社の情報セキュリティポリシー（ツール3-2回  
脅威一覧）](#)

1.6.1.7. [◦付録3回わが社の情報セキュリティポリシー（ツール3-3回  
対策状況チェックシート）](#)

1.6.1.8. [◦付録3回わが社の情報セキュリティポリシー（ツール3-4回  
情報セキュリティポリシーサンプル）](#)

1.6.1.9. [◦付録4回情報セキュリティ関連ガイド・法令一覧](#)

1.6.1.10. [◦付録5回情報セキュリティ相談窓口](#)

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

1.6.3. [●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's diary](#)

1.6.4. [●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's  
diary](#)

1.6.5. [●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's diary](#)

1.7. 家庭個人向け


## 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's diary【更新中】 

### [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's diary【更新中】](#)

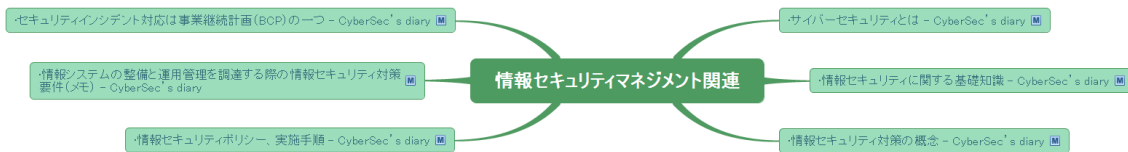
## 1.8. 重要インフラ関連

## 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's diary【更新中】 

### [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's diary【更新中】](#)

## 1.9. 情報セキュリティマネジメント関連



### [1.9.1. サイバーセキュリティとは - CyberSec's diary](#)

### [1.9.2. 情報セキュリティに関する基礎知識 - CyberSec's diary](#)

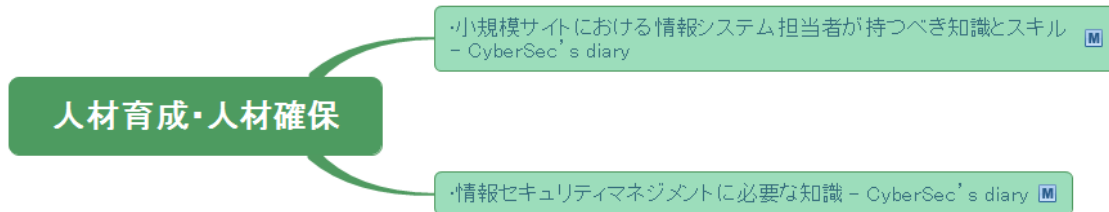
### [1.9.3. 情報セキュリティ対策の概念 - CyberSec's diary](#)

### [1.9.4. 情報セキュリティポリシー、実施手順 - CyberSec's diary](#)

### [1.9.5. 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's diary](#)

1.9.6. [●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's diary](#)

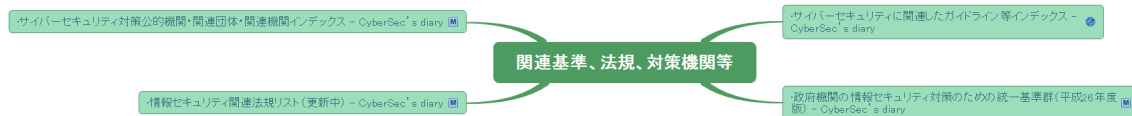
1.10. 人材育成・人材確保



1.10.1. [●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's diary](#)

1.10.2. [●情報セキュリティマネジメントに必要な知識 - CyberSec's diary](#)

1.11. 関連基準、法規、対策機関等




1.11.1. [●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's diary](#)



1.11.1.1. ○公的機関、教育機関向け、個人ユーザー向け、事業者向け

1.11.2. [●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's 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's diary 

・全体的内容、規定の趣旨、対策例


1.11.2.1. ◦全体的内容、規定の趣旨、対策例

1.11.3. [・情報セキュリティ関連法規リスト\(更新中\) - CyberSec's diary](#)

1.11.4. [・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's diary](#)

1.12. セキュリティ関連情報提供サイト一覧


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's diary 

1.12.1. [・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's diary](#)

1.13. ニュース

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】 

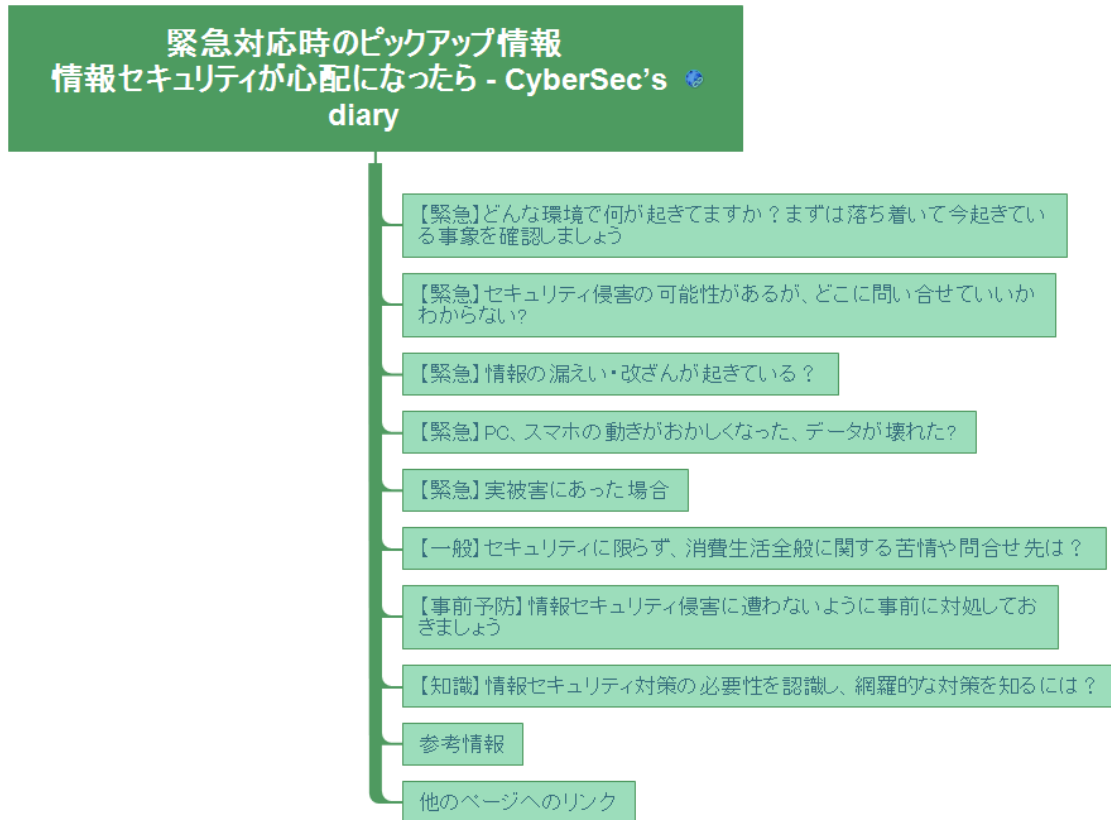
・「中小企業サイバーセキュリティ対策相談窓口」の開設 - CyberSec's diary 

1.13.1. [・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】](#)

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

## 2. [緊急対応時のピックアップ情報](#)

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



### 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



#### 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】\(pdf形式\)](#)

・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。漠然とした不安の中で相談をする際に、今自分や企業がこ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。

3.1.1.1. ◦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、今自分や企業がこ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。

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

【緊急】セキュリティ侵害の可能性があるが、どこに問い合わ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

3.2.1. ◦「[中小企業サイバーセキュリティ対策相談窓口](#)」へ

☎ 03-5320-4773

・「中小企業サイバーセキュリティ対策相談窓口」へ

3.2.1.1. ☎ 03-5320-4773

3.3. 【緊急】情報の漏えい・改ざんが起きている？

【緊急】情報の漏えい・改ざんが起きている？

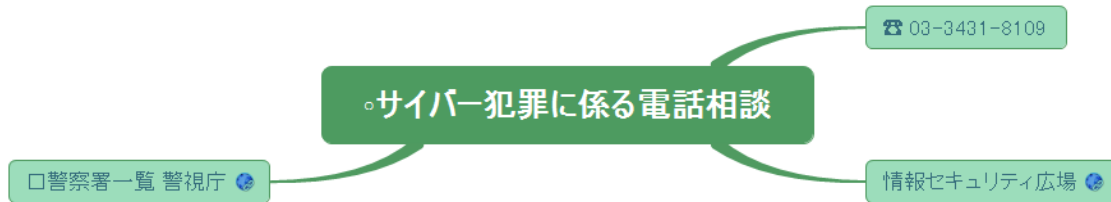
・犯罪の可能性がある場合は、警視庁へ

3.3.1. ◦犯罪の可能性がある場合は、警視庁へ

・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

### 3.3.1.1. サイバー犯罪に係る電話相談



#### 3.3.1.1.1. ☎ 03-3431-8109

#### 3.3.1.1.2. [情報セキュリティ広場](#)

#### 3.3.1.1.3. [📍警察署一覧 警視庁](#)

### 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?

【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

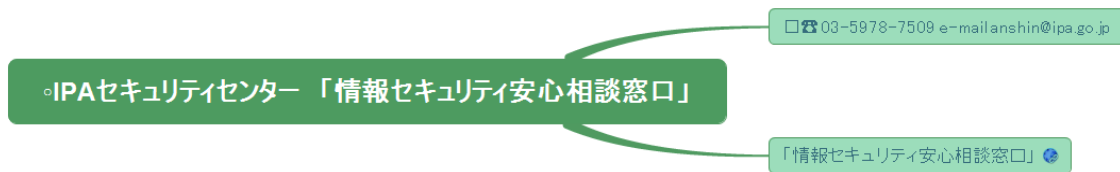
#### 3.4.1. ウイルス感染、不正アクセスの可能性

・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」

#### 3.4.1.1. ・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」





3.4.1.1.1. ☎ 03-5978-7509 e-mail anshin@ipa.go.jp

3.4.1.1.2. [「情報セキュリティ安心相談窓口」](#)

### 3.5. 【緊急】実被害にあった場合



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。

3.5.2. •ウイルス・不正アクセス届出



3.5.2.1. [IPAセキュリティセンター](#)



3.5.2.1.1. ☎ 03-3518-2177

### 3.5.3. •インシデント報告・届出

#### •インシデント報告・届出

◦JPCERT コーディネーションセンター 

#### 3.5.3.1. ◦JPCERT コーディネーションセンター


☎03-3518-2177

#### ◦JPCERT コーディネーションセンター


##### 3.5.3.1.1. ☎03-3518-2177

### 3.5.4. •サイバー犯罪届出（全国）

#### •サイバー犯罪届出(全国)

◦「警察庁 サイバー犯罪対策」 

#### 3.5.4.1. ◦「警察庁」サイバー犯罪対策」

◦都道府県警察本部のサイバー犯罪相談窓口等一覧 

#### ◦「警察庁 サイバー犯罪対策」

##### 3.5.4.1.1. ◦都道府県警察本部のサイバー犯罪相談窓口等一覧

3.6. 【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？

【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

・暮らしにかかわる東京都の情報サイト

### 3.6.1. [・消費者ホットライン](#)

☎188

・消費者ホットライン

#### 3.6.1.1. ☎188

### 3.6.2. [・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 東京暮らしWEB

・暮らしにかかわる東京都の情報サイト

・消費生活相談窓口のご案内 | 東京暮らしWEB

#### 3.6.2.1. [・東京都の消費生活総合サイト 東京暮らしWEB](#)

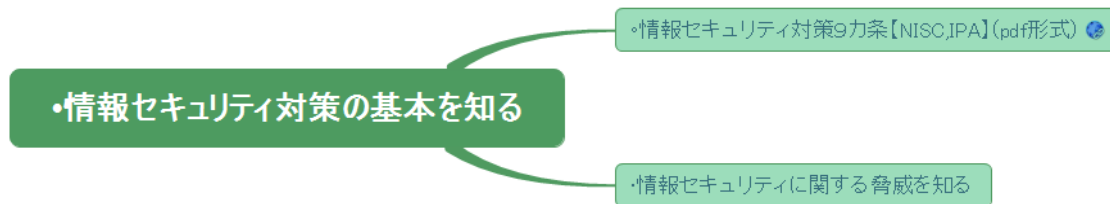
#### 3.6.2.2. [・消費生活相談窓口のご案内 | 東京暮らしWEB](#)

3.7. 【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

【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

### 3.7.1. [・情報セキュリティ対策の基本を知る](#)

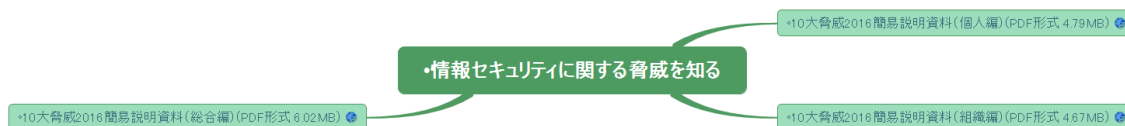


### 3.7.1.1. [情報セキュリティ対策9カ条【NISC,IPA】\(pdf形式\)](#)



3.7.1.1.1. [ロイ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](#)

### 3.7.1.2. [情報セキュリティに関する脅威を知る](#)

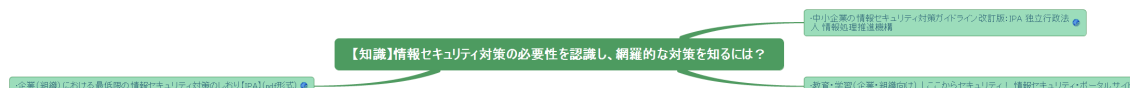


#### 3.7.1.2.1. [10大脅威2016簡易説明資料\(個人編\)\(PDF形式 4.79MB\)](#)

#### 3.7.1.2.2. [10大脅威2016簡易説明資料\(組織編\)\(PDF形式 4.67MB\)](#)

#### 3.7.1.2.3. [10大脅威2016簡易説明資料\(総合編\)\(PDF形式 6.02MB\)](#)

3.8. 【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？



### 3.8.1. [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](#)

・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

・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。

3.8.1.1. ◦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。

3.8.2. •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

・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

・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

3.8.2.1. ◦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

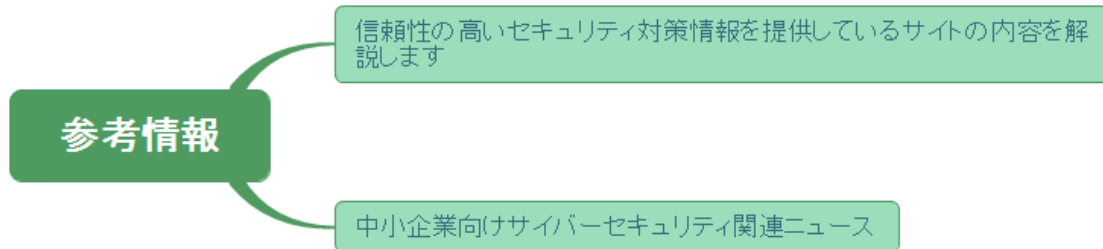
3.8.3. •企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】（pdf形式）

・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、従業員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。

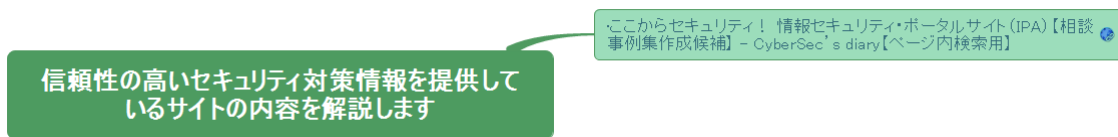
・企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】（pdf形式）

3.8.3.1. ◦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、従業員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。

### 3.9. 参考情報



### 3.9.1. 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を解説します



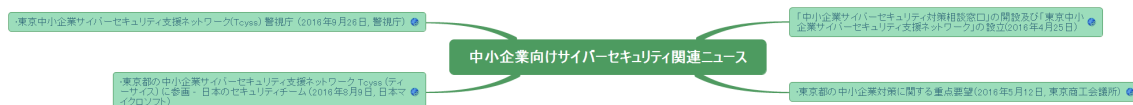
#### 3.9.1.1. [●ここからセキュリティ！](#)

[情報セキュリティ・ポータルサイト \(IPA\) 【相談事例集作成候補】 - CyberSec's diary 【ページ内検索用】](#)



#### 3.9.1.1.1. 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、また必要に応じて内容の解説を加えたもの。

### 3.9.2. 中小企業向けサイバーセキュリティ関連ニュース



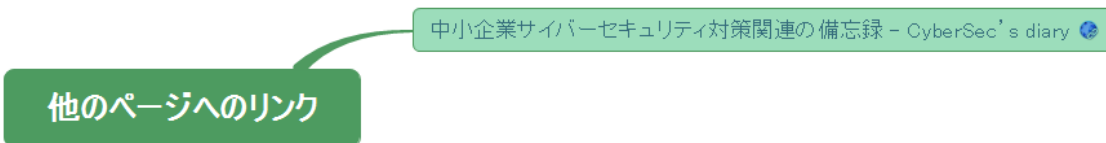
#### 3.9.2.1. [「中小企業サイバーセキュリティ対策相談窓口」の開設及び「東京中小企業サイバーセキュリティ支援ネットワーク」の設立\(2016年4月25日\)](#)

3.9.2.2. [●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）](#)

3.9.2.3. [●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 \(ティーサイズ\) 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）](#)

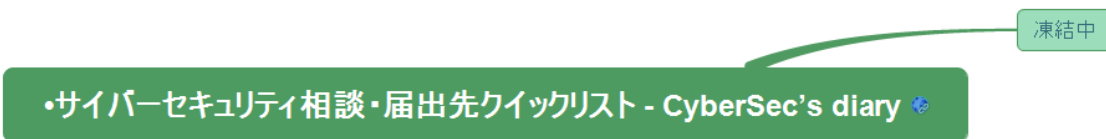
3.9.2.4. [●東京中小企業サイバーセキュリティ支援ネットワーク \(Tcyss\) 警視庁（2016年9月26日, 警視庁）](#)

### 3.10. 他のページへのリンク



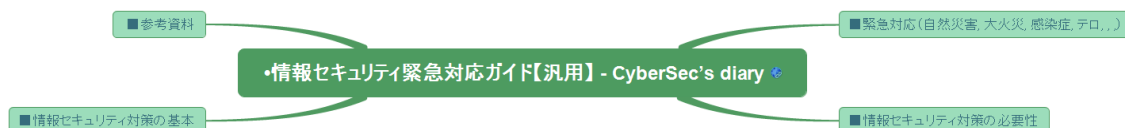
3.10.1. [中小企業サイバーセキュリティ対策関連の備忘録 - CyberSec's diary](#)

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



### 4.1. 凍結中

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

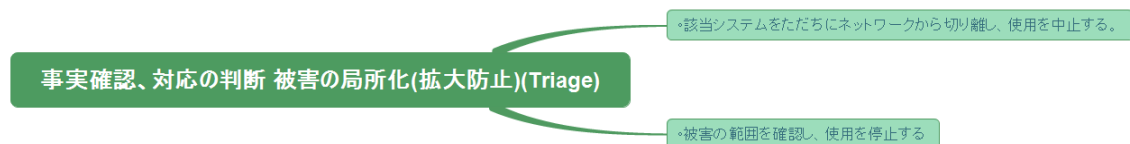


## 5.1. ■緊急対応（自然災害, 大火災, 感染症, テロ,,,）



### 5.1.1. 事象の検知、報告受付(Detect)

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



5.1.2.1. ・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。

5.1.2.2. ・被害の範囲を確認し、使用を停止する

### 5.1.3. 緊急連絡



5.1.3.1. ・システム管理者、関係部署、関係機関に連絡。指示に従う。

5.1.3.2. ・犯罪の可能性⇒警視庁

5.1.3.3. ・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

### 5.1.4. 原状保全



## 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

5.1.4.1. ◦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

### 5.1.5. 原因調査

#### 原因調査

◦なぜ情報セキュリティ侵害が起きたか？

◦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。

◦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

5.1.5.1. ◦なぜ情報セキュリティ侵害が起きたか？

5.1.5.2. ◦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

5.1.5.3. ◦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。

### 5.1.6. 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。

#### 早期復旧・事業継続 (Respond)

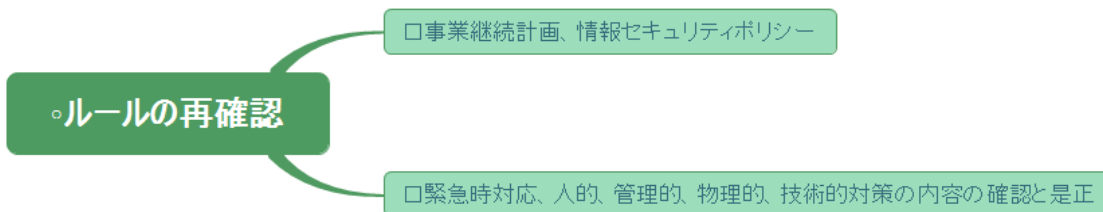
5.1.6.1. ◦確認できた事象に対する再発防止のための改善策を、システム管理者の指示に従って、適切な復旧を行う。

### 5.1.7. 恒久的対策（再発防止策）



#### 5.1.7.1. インシデントからの知見の学習

#### 5.1.7.2. ルールの再確認



##### 5.1.7.2.1. 事業継続計画、情報セキュリティポリシー

##### 5.1.7.2.2. 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



5.1.7.2.2.1. 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。

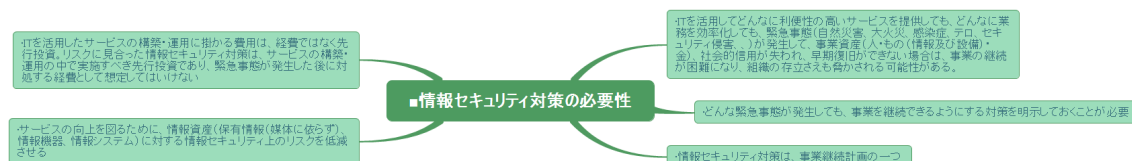
5.1.7.2.2.2. 最低限守るべきルールを明確にして、それを守らせることが重要。

#### 5.1.8. 通常運用



#### 5.1.8.1. 平時からの実施状況の確認（監査）

### 5.2. ■情報セキュリティ対策の必要性



**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。**

**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**

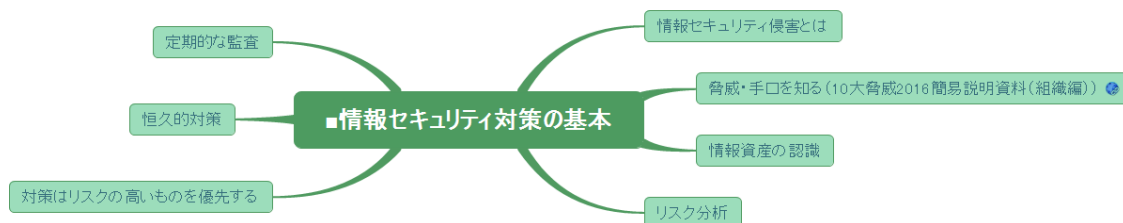
**5.2.3. •情報セキュリティ対策は、事業継続計画の一つ**

**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**

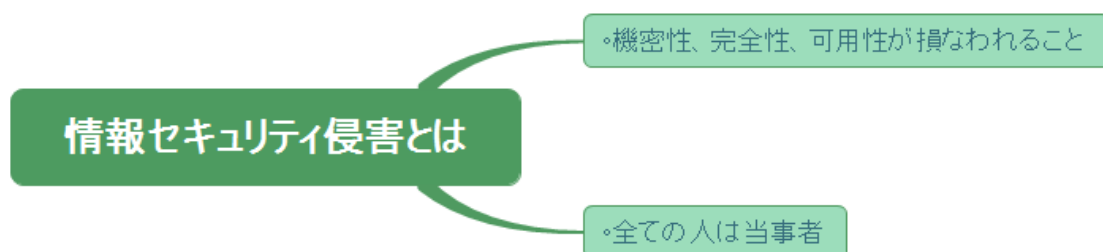
**5.2.5. •ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用**

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

### 5.3. ■情報セキュリティ対策の基本

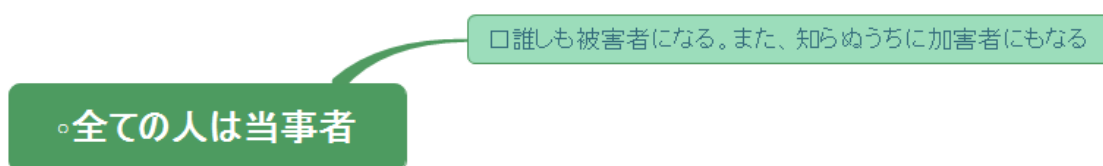


#### 5.3.1. 情報セキュリティ侵害とは



##### 5.3.1.1. ・機密性、完全性、可用性が損なわれること

##### 5.3.1.2. ・全ての人は当事者

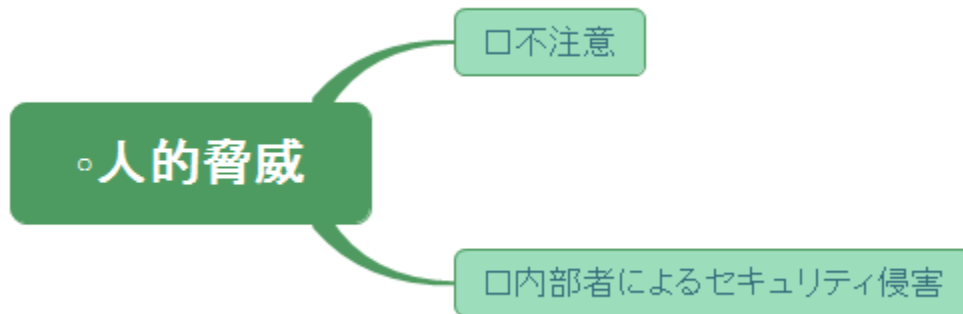


##### 5.3.1.2.1. □誰しも被害者になる。また、知らぬうちに加害者にもなる

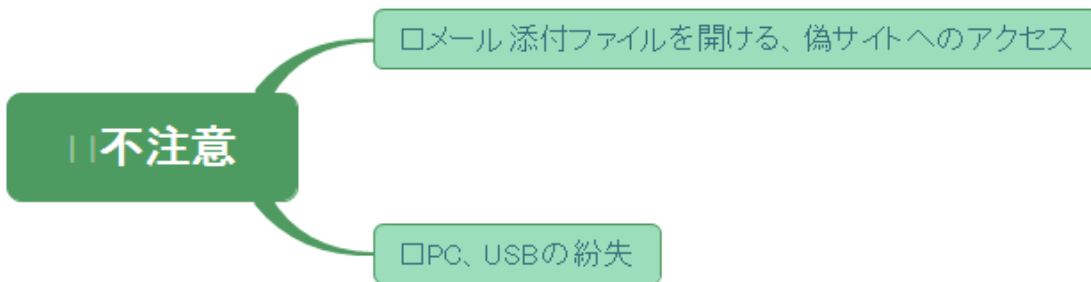
#### 5.3.2. [脅威・手口を知る（10大脅威2016簡易説明資料（組織編））](#)



#### 5.3.2.1. 人的脅威



##### 5.3.2.1.1. 不注意



###### 5.3.2.1.1.1. メール添付ファイルを開ける、偽サイトへのアクセス

###### 5.3.2.1.1.2. PC、USBの紛失

##### 5.3.2.1.2. 内部者によるセキュリティ侵害



###### 5.3.2.1.2.1. 情報の持ち出し、不正アクセス

#### 5.3.2.2. 正規のウェブサイトを改ざん

#### 5.3.2.3. ウェブサイトにアクセスするだけでマルウェア感染

#### 5.3.2.4. 標的型メールでの不正サイトへの誘導

#### 5.3.2.5. 不審なメールのマルウェア添付

### 5.3.3. 情報資産の認識

#### 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

5.3.3.1. 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

### 5.3.4. リスク分析

#### 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）

5.3.4.1. 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）

### 5.3.5. 対策はリスクの高いものを優先する



5.3.5.1. ◦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

5.3.5.2. ◦重要度の高いファイルのバックアップ

5.3.5.3. ◦ソフトウェアの更新

5.3.5.4. ◦マルウェア（ウイルス等）対策ソフトの導入

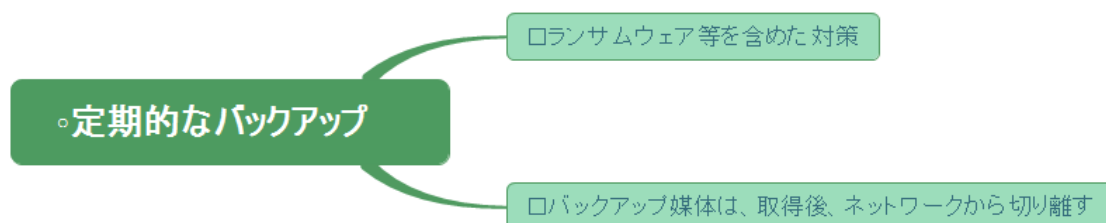
5.3.5.5. ◦パスワード・認証の強化

5.3.5.6. ◦設定の見直し（ルータ、PC等）

### 5.3.6. 恒久的対策



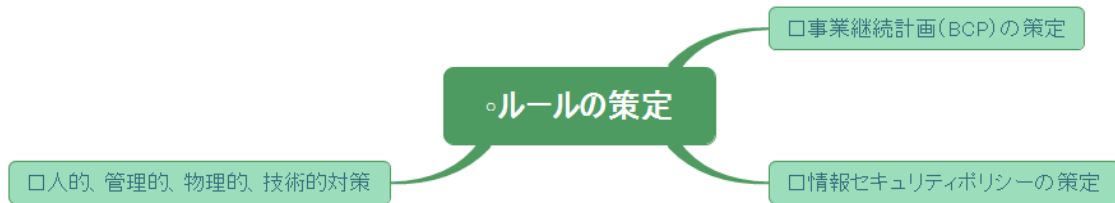
#### 5.3.6.1. ◦定期的なバックアップ ㊦



##### 5.3.6.1.1. ㊦ランサムウェア等を含めた対策

##### 5.3.6.1.2. ㊦バックアップ媒体は、取得後、ネットワークから切り離す

#### 5.3.6.2. ◦ルール of 策定

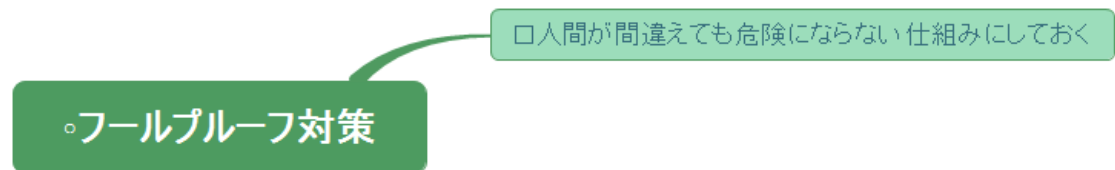


##### 5.3.6.2.1. ◻事業継続計画（BCP） of 策定

##### 5.3.6.2.2. ◻情報セキュリティポリシー of 策定

##### 5.3.6.2.3. ◻人的、管理的、物理的、技術的対策

#### 5.3.6.3. ◦フールプルーフ対策



##### 5.3.6.3.1. ◻人間が間違えても危険にならない仕組みにしておく

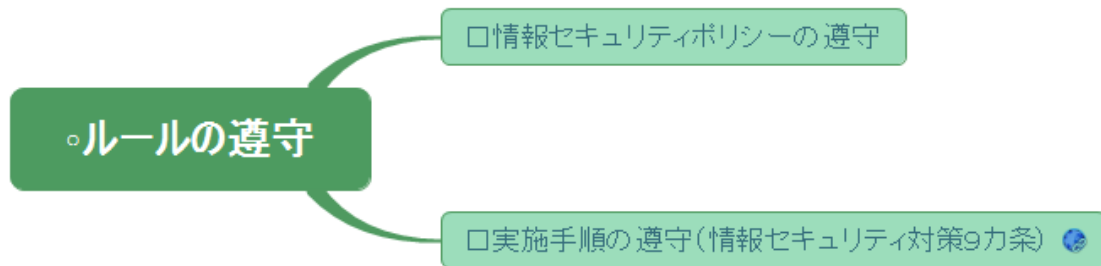
#### 5.3.6.4. ◦フェールセーフ対策



##### 5.3.6.4.1. ◻機械が壊れても危険にならない仕組みにしておく

#### 5.3.6.5. ◦ルール of 遵守





#### 5.3.6.5.1. ④情報セキュリティポリシーの遵守

#### 5.3.6.5.2. ④実施手順の遵守 (情報セキュリティ対策9カ条)



##### 5.3.6.5.2.1. ④OSやソフトウェアは常に最新の状態に

##### 5.3.6.5.2.2. ④パスワードは貴重品のように管理

##### 5.3.6.5.2.3. ④ログインID・パスワードは絶対に教えない

##### 5.3.6.5.2.4. ④身に覚えのないファイルは開かない

##### 5.3.6.5.2.5. ④ウイルス対策ソフトを導入

##### 5.3.6.5.2.6. ④ネットショッピングは信頼できるお店で

##### 5.3.6.5.2.7. ④大切な情報は失う前に複製

##### 5.3.6.5.2.8. ④外出先では紛失・盗難に注意

##### 5.3.6.5.2.9. ④困ったときは一人で悩まず相談を

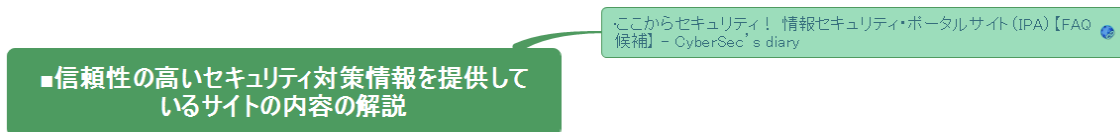
### 5.3.7. 定期的な監査

### 5.4. ■参考資料

## 6. ●相談対応の手引きレファレンスリスト【相談員用】 - CyberSec's diary

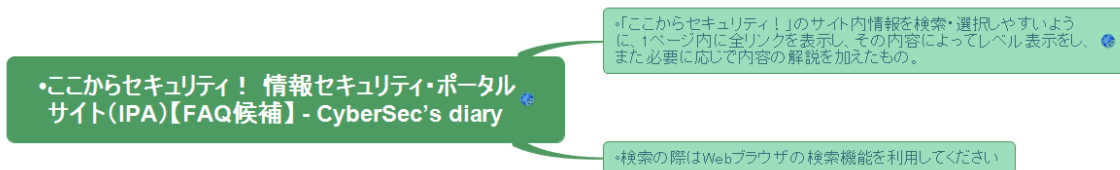


### 6.1. ■信頼性の高いセキュリティ対策情報を提供しているサイトの内容の解説



#### 6.1.1. ●ここからセキュリティ！

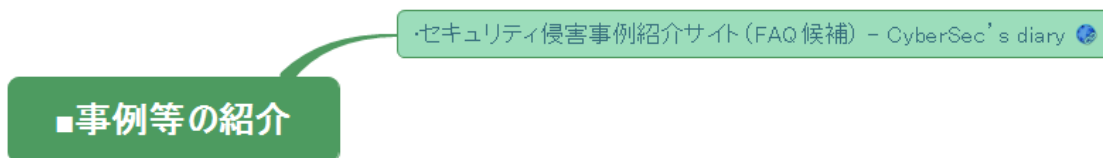
#### 情報セキュリティ・ポータルサイト (IPA)【FAQ候補】 - CyberSec's diary



6.1.1.1. 。「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、また必要に応じて内容の解説を加えたもの。

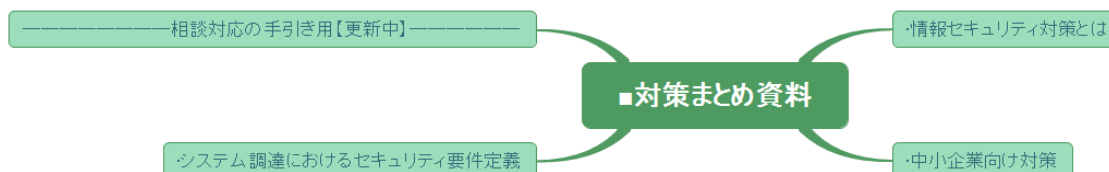
6.1.1.2. 検索の際はWebブラウザの検索機能を利用してください

### 6.2. ■事例等の紹介

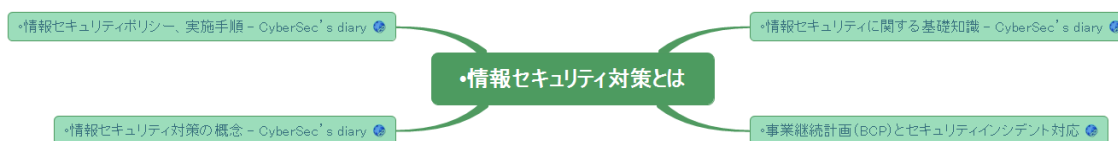


#### 6.2.1. [・セキュリティ侵害事例紹介サイト \(FAQ候補\) - CyberSec's diary](#)

### 6.3. ■対策まとめ資料



#### 6.3.1. •情報セキュリティ対策とは



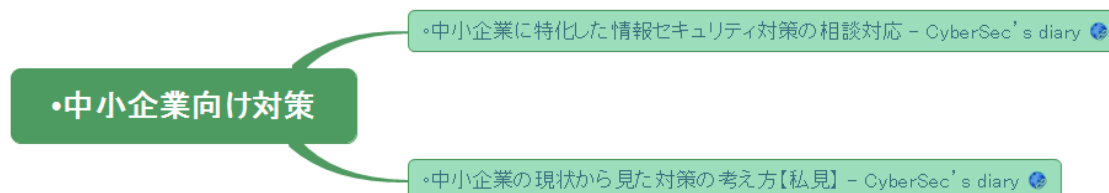
##### 6.3.1.1. [情報セキュリティに関する基礎知識 - CyberSec's diary](#)

##### 6.3.1.2. [事業継続計画 \(BCP\) とセキュリティインシデント対応](#)

##### 6.3.1.3. [情報セキュリティ対策の概念 - CyberSec's diary](#)

##### 6.3.1.4. [情報セキュリティポリシー、実施手順 - CyberSec's diary](#)

#### 6.3.2. •中小企業向け対策



6.3.2.1. [◦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's diary](#)

6.3.2.2. [◦中小企業の現状から見た対策の考え方【私見】 - CyberSec's diary](#)

6.3.3. ●システム調達におけるセキュリティ要件定義

●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's diary

6.3.3.1. [◦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's diary](#)

6.3.4. —————相談対応の手引き用【更新中】—————

—————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's diary

【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's diary

6.3.4.1. [【更新中】情報セキュリティ緊急対応ガイド【汎用】 - CyberSec's diary](#)

6.3.4.2. ● [【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's diary](#)

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

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

サイバーセキュリティ対策相談対応の手引き(メモ)

7.1. ●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

## ・サイバーセキュリティ対策相談対応の手引き(メモ)

### 7.1.1. 展開した文書

## 8. [・セキュリティ侵害事例紹介サイト \(FAQ候補\) - CyberSec's diary](#)

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

各種Webから抜粋したページ

・相談窓口対応事例(FAQ候補) - CyberSec's diary

### 8.1. 各種Webから抜粋したページ

### 8.2. [相談窓口対応事例 \(FAQ候補\) - CyberSec's diary](#)

## 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's diary](#)

・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's diary

「ここからセキュリティ」を展開したページ

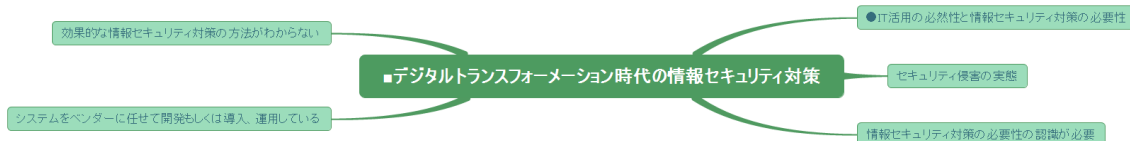
### 9.1. 「ここからセキュリティ」を展開したページ

## 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】](#)

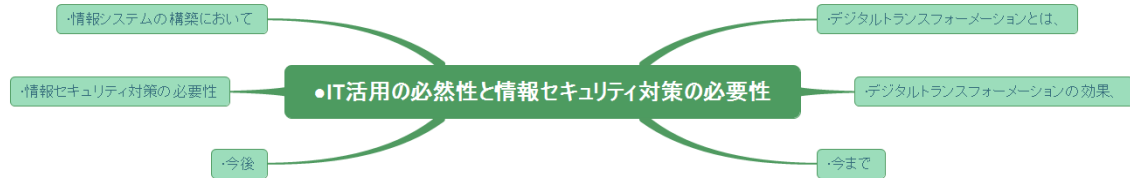
・IT化・デジタル化により業務の効率化・サービスの向上を図るために、セキュリティ対策を実施【私見】

■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

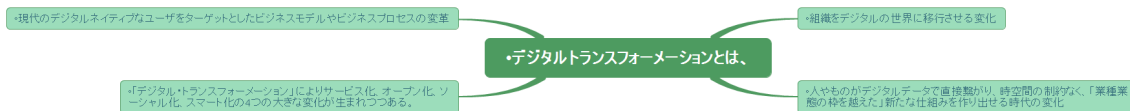
## 10.1. ■デジタルトランスフォーメーション時代の情報セキュリティ対策



### 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



#### 10.1.1.1. ●デジタルトランスフォーメーションとは、

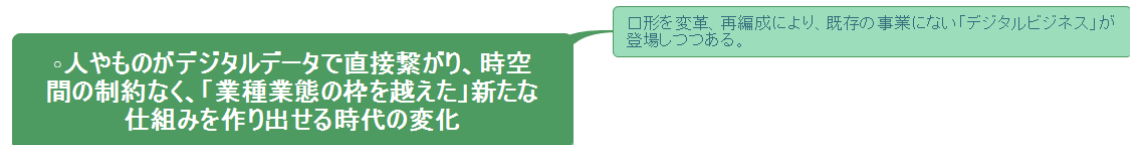


##### 10.1.1.1.1. ◦組織をデジタルの世界に移行させる変化



10.1.1.1.1.1. 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

10.1.1.1.2. ◦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



10.1.1.1.2.1. 図形を変革、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。

10.1.1.1.3. ◦「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。

10.1.1.1.4. ◦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

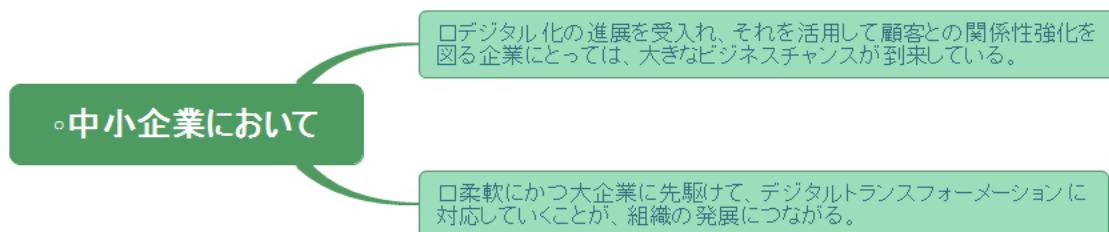
10.1.1.2. •デジタルトランスフォーメーションの効果、



10.1.1.2.1. ◦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。

10.1.1.2.2. ◦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。

10.1.1.2.3. ◦中小企業において



10.1.1.2.3.1. 図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。

10.1.1.2.3.2. ②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。

10.1.1.3. •今まで



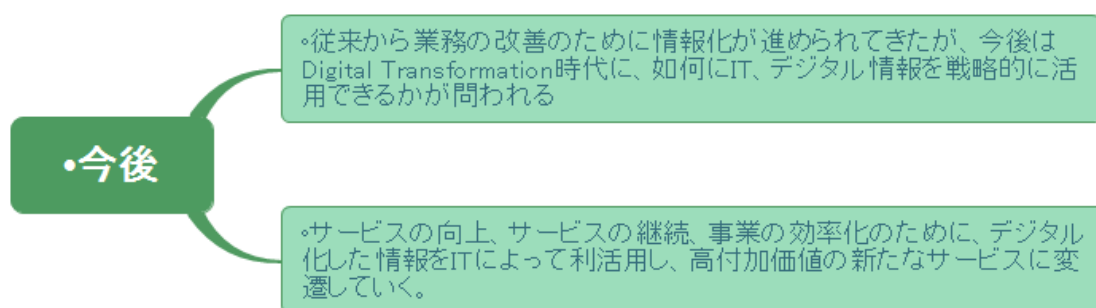
10.1.1.3.1. ◦これまで企業のITシステムは、業務、生産工程等を効率化して、経営を安定化させることに重きが置かれてきた。

10.1.1.3.2. ◦単なる効率化だけではビジネスの競争に勝ち残れない

10.1.1.3.3. ◦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

10.1.1.3.4. ◦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

10.1.1.4. •今後

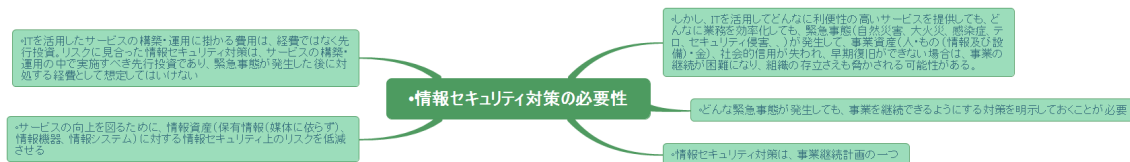


10.1.1.4.1. ◦従来から業務の改善のために情報化が進められてきたが、今後はDigital Transformation時代に、如何にIT、デジタル情報を戦略的に活用できるかが問われる



**10.1.1.4.2.** ◦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。

#### 10.1.1.5. •情報セキュリティ対策の必要性



**10.1.1.5.1.** ◦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。

**10.1.1.5.2.** ◦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

**10.1.1.5.3.** ◦情報セキュリティ対策は、事業継続計画の一つ

**10.1.1.5.4.** ◦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

**10.1.1.5.5.** ◦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

#### 10.1.1.6. •情報システムの構築において

## ・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

**10.1.1.6.1.** 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

## 10.1.2. セキュリティ侵害の実態

### 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)

・個人情報漏えい媒体、経路(2013年 NPO日本ネットワーク協会)

### 10.1.2.1. ・「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)



**10.1.2.1.1.** ・誤操作34.9%

**10.1.2.1.2.** ・管理ミス32.3%

**10.1.2.1.3.** ・紛失・置忘れ14.3%

**10.1.2.1.4.** ・盗難5.5%

**10.1.2.1.5.** ・不正アクセス4.7%

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



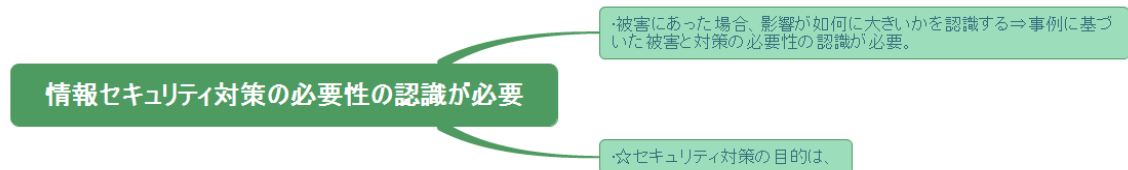
#### 10.1.2.2.1. ○●紙媒体58.7%

#### 10.1.2.2.2. ○●USB等記憶媒体25.9%

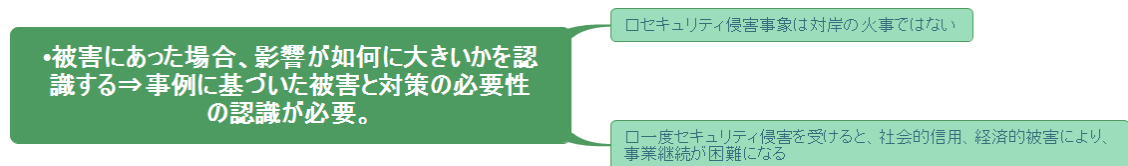
#### 10.1.2.2.3. ○●電子メール5.5%

#### 10.1.2.2.4. ○●インターネット5.0%

### 10.1.3. 情報セキュリティ対策の必要性の認識が必要



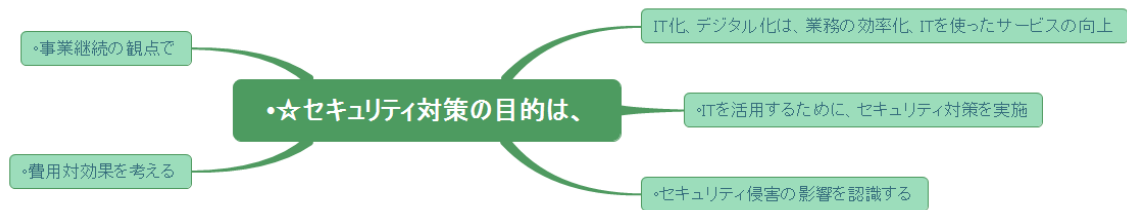
#### 10.1.3.1. ●被害にあった場合、影響が如何に大きいかを認識する⇒事例に基づいた被害と対策の必要性の認識が必要。



##### 10.1.3.1.1. □セキュリティ侵害事象は対岸の火事ではない

##### 10.1.3.1.2. □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

#### 10.1.3.2. ●☆セキュリティ対策の目的は、



#### 10.1.3.2.1. 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



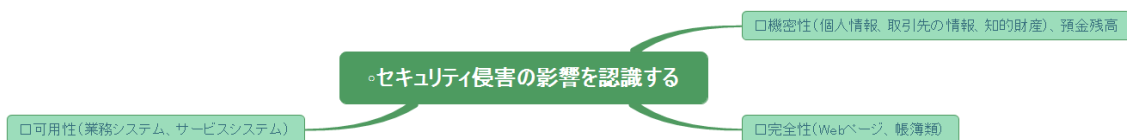
##### 10.1.3.2.1.1. ㊦どんな優れたサービスも、セキュリティに不安があるサービスは利用されない

#### 10.1.3.2.2. ㊦ITを活用するために、セキュリティ対策を実施



##### 10.1.3.2.2.1. ㊦（自動車を運転するために、自動車保険に入る）

#### 10.1.3.2.3. ㊦セキュリティ侵害の影響を認識する

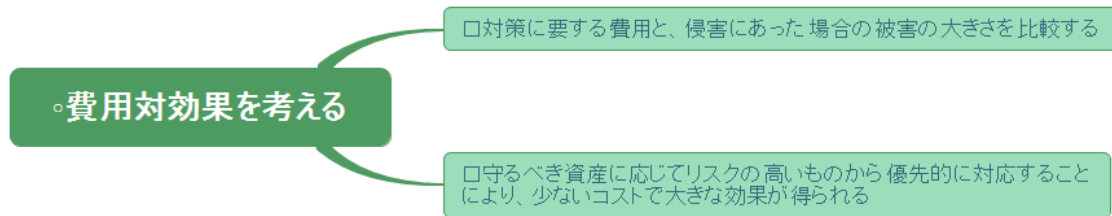


##### 10.1.3.2.3.1. ㊦機密性（個人情報、取引先の情報、知的財産）、預金残高

##### 10.1.3.2.3.2. ㊦完全性（Webページ、帳簿類）

##### 10.1.3.2.3.3. ㊦可用性（業務システム、サービスシステム）

#### 10.1.3.2.4. ◦費用対効果を考える



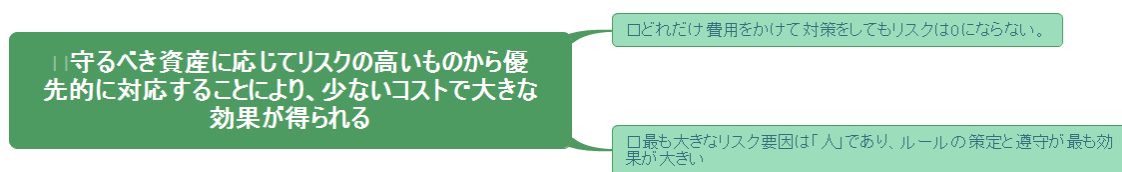
##### 10.1.3.2.4.1. ②対策に要する費用と、侵害にあった場合の被害の大きさを比較する



10.1.3.2.4.1.1.②自動車任意保険、火災保険のようなもの。

10.1.3.2.4.1.2.②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

##### 10.1.3.2.4.2. ③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



10.1.3.2.4.2.1.③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。

10.1.3.2.4.2.2.③最も大きなリスク要因は「人」であり、ルール策定と遵守が最も効果大きい

#### 10.1.3.2.5. ◦事業継続の観点で

## 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

### 10.1.3.2.5.1. □経済的損失、社会的信用の喪失⇒事業存続、事業継続の危機

### 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

・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

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

#### 10.1.4.1. •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

### 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

・認識すること

効果的な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

#### 10.1.5.1. •認識すること

・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

・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る

・どれだけお金を掛けても脆弱性はゼロにはならない

・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

##### 10.1.5.1.1. •断片的な対策では、セキュリティホールはなくなる

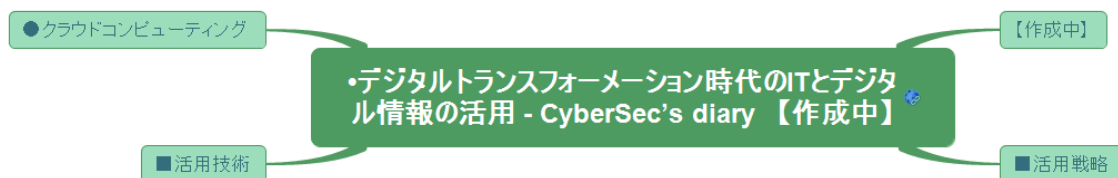
##### 10.1.5.1.2. •内部職員による故意もしくは過失によるセキュリティ侵害は全体の80%以上

##### 10.1.5.1.3. •どれだけお金を掛けても脆弱性はゼロにはならない

10.1.5.1.4. ◦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

10.1.5.2. •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

## 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's diary 【作成中】



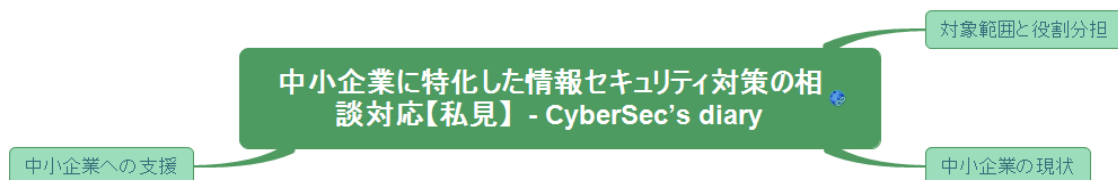
11.1. 【作成中】

11.2. ■活用戦略

11.3. ■活用技術

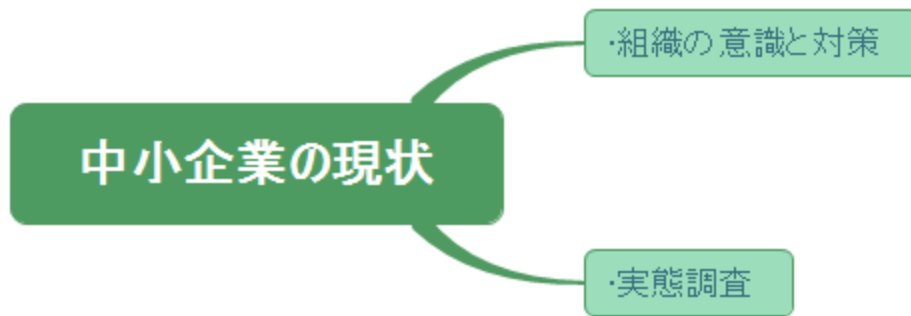
11.4. •クラウドコンピューティング

## 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's diary



12.1. 対象範囲と役割分担

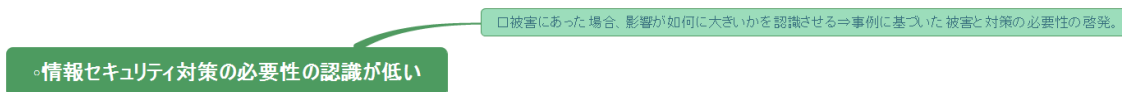
12.2. 中小企業の現状



### 12.2.1. 組織の意識と対策



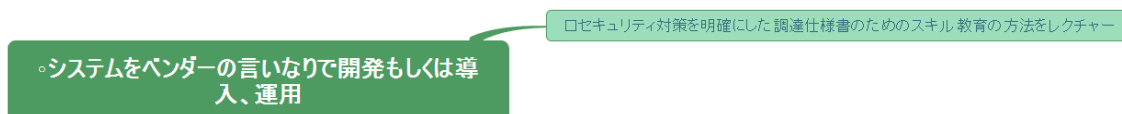
#### 12.2.1.1. 情報セキュリティ対策の必要性の認識が低い



##### 12.2.1.1.1.

☑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。

#### 12.2.1.2. 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



##### 12.2.1.2.1.

☑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

#### 12.2.1.3. 情報セキュリティ対策の方法がわからない



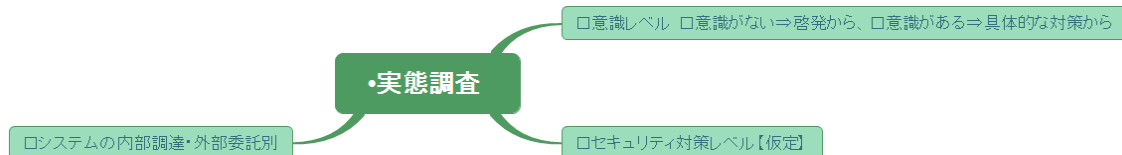
◦情報セキュリティ対策の方法がわからない

□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

#### 12.2.1.3.1.

□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

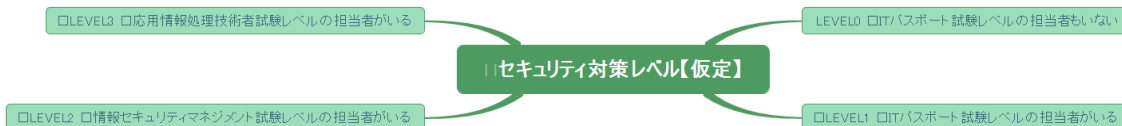
#### 12.2.2. •実態調査



##### 12.2.2.1. □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

##### 12.2.2.2. □セキュリティ対策レベル【仮定】



##### 12.2.2.2.1. LEVEL0 □ITパスポート試験レベルの担当者もいない

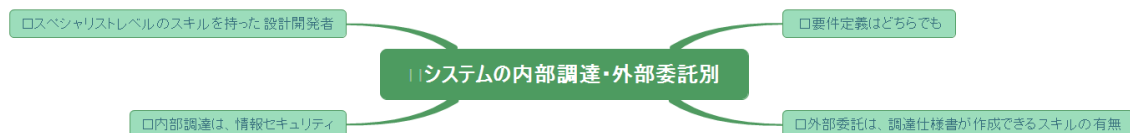
##### 12.2.2.2.2. □LEVEL1 □ITパスポート試験レベルの担当者がいる

##### 12.2.2.2.3. □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

##### 12.2.2.2.4. □LEVEL3 □応用情報処理技術者試験レベルの担当者がいる

#### 12.2.2.3. □システムの内部調達・外部委託別



12.2.2.3.1. □要件定義はどちらでも

12.2.2.3.2. □外部委託は、調達仕様書が作成できるスキルの有無

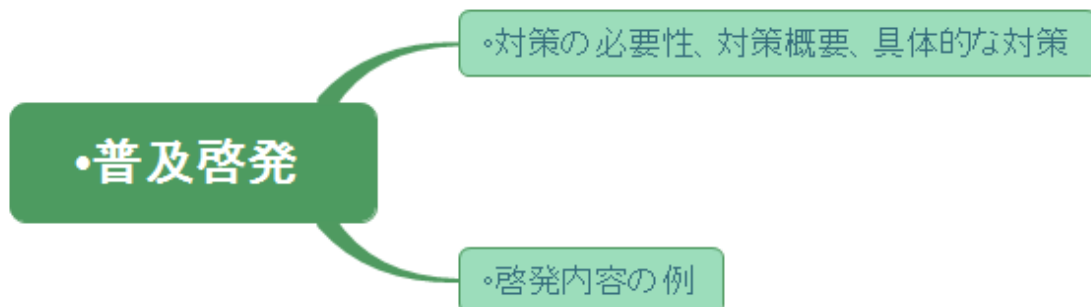
12.2.2.3.3. □内部調達は、情報セキュリティ

12.2.2.3.4. □スペシャリストレベルのスキルを持った設計開発者

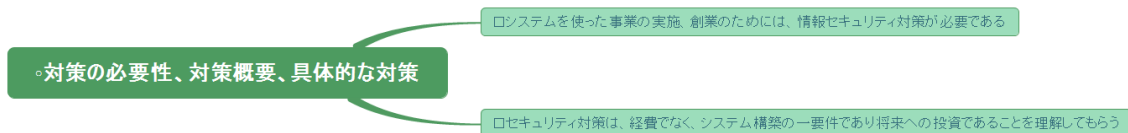
## 12.3. 中小企業への支援



### 12.3.1. ・普及啓発



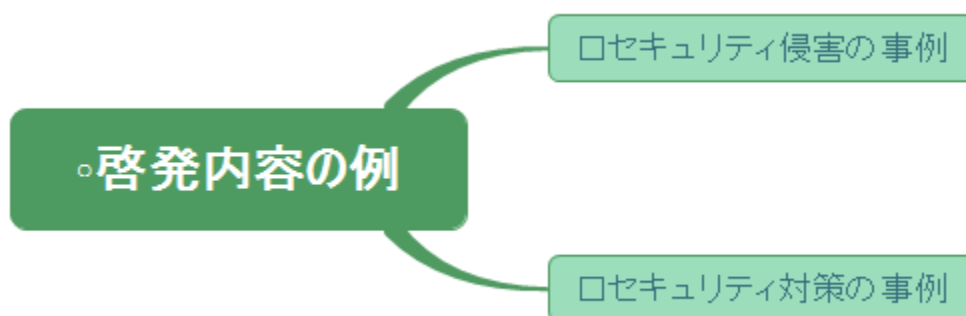
12.3.1.1. ◦対策の必要性、対策概要、具体的な対策



12.3.1.1.1. ④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

12.3.1.1.2. ④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

12.3.1.2. ○啓発内容の例



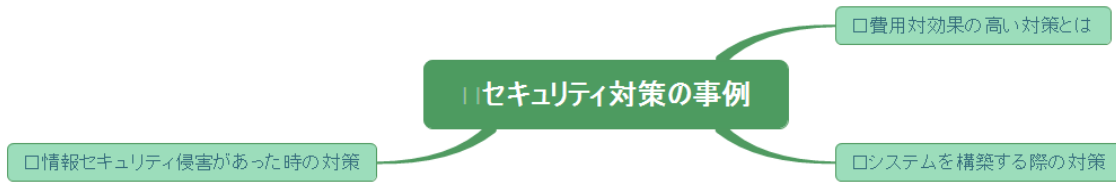
12.3.1.2.1. ④セキュリティ侵害の事例



12.3.1.2.1.1. ④脅威の事例

12.3.1.2.1.2. ④リスクの事例

#### 12.3.1.2.2. ④セキュリティ対策の事例



##### 12.3.1.2.2.1. ④費用対効果の高い対策とは

##### 12.3.1.2.2.2. ④システムを構築する際の対策

##### 12.3.1.2.2.3. ④情報セキュリティ侵害があった時の対策

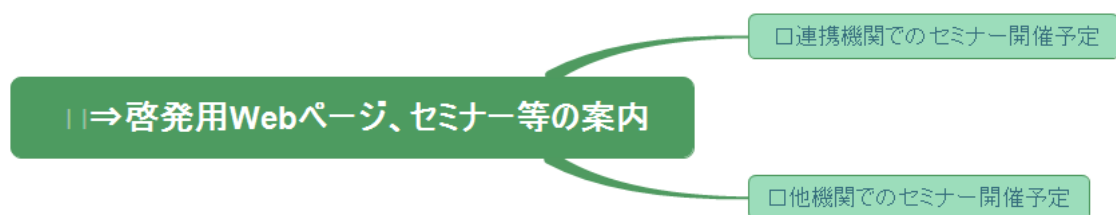
#### 12.3.2. •対策の概要



##### 12.3.2.1. •セキュリティ対策の普及啓発



##### 12.3.2.1.1. ④⇒啓発用Webページ、セミナー等の案内



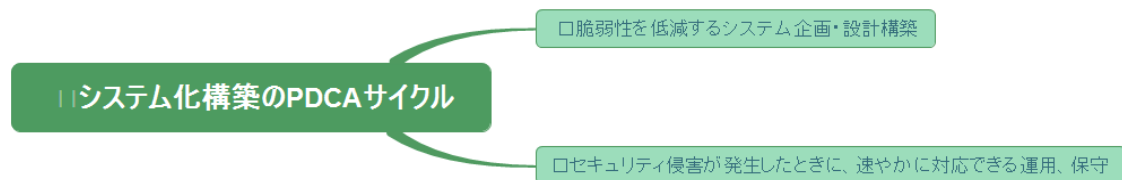
##### 12.3.2.1.1.1. ④連携機関でのセミナー開催予定

#### 12.3.2.1.1.2. ②他機関でのセミナー開催予定

### 12.3.2.2. ①セキュリティの予防対策



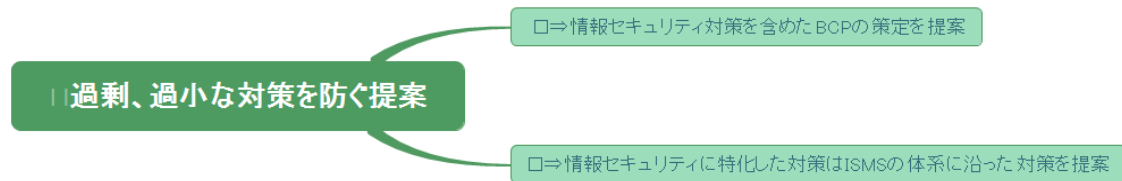
#### 12.3.2.2.1. ②システム化構築のPDCAサイクル



##### 12.3.2.2.1.1. ②脆弱性を低減するシステム企画・設計構築

12.3.2.2.1.2. ②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

#### 12.3.2.2.2. ②過剰、過小な対策を防ぐ提案



##### 12.3.2.2.2.1. ②⇒情報セキュリティ対策を含めたBCPの策定を提案

12.3.2.2.2.2. ②⇒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

#### 12.3.2.2.3. ②重大事象を優先的に対策 ②重要の情報資産は何か

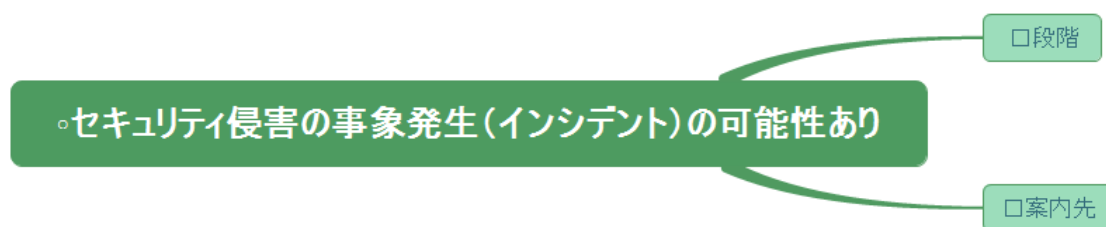


12.3.2.2.3.1. □重要な情報資産への頻度の高い脅威の洗い出し

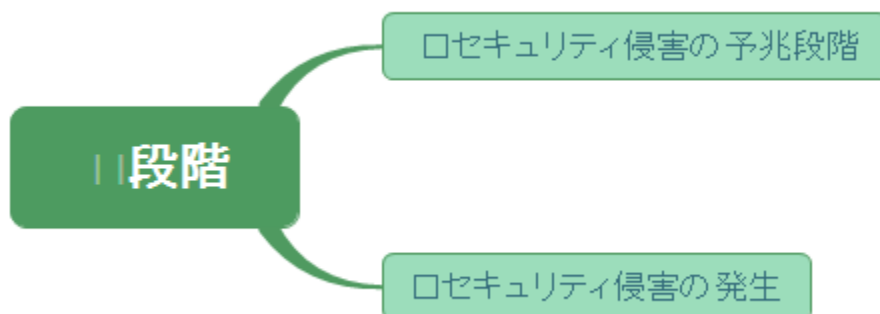
12.3.2.2.3.2. □脅威に対する脆弱性の度合い

12.3.2.2.3.3. □脆弱性を低減させる対策は？

12.3.2.3. ◦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



12.3.2.3.1. □段階



12.3.2.3.1.1. □セキュリティ侵害の予兆段階

12.3.2.3.1.2. □セキュリティ侵害の発生

12.3.2.3.2. □案内先



#### 12.3.2.3.2.1. 犯罪の可能性

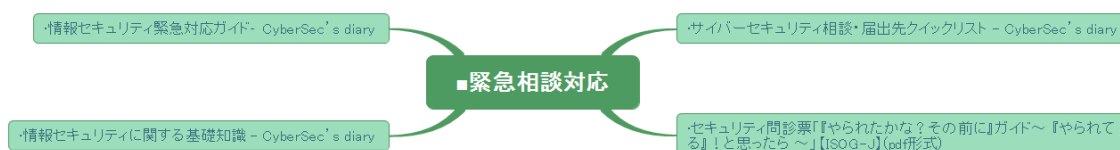
#### 12.3.2.3.2.2. 一般的な不正アクセス、ウイルス感染

#### 12.3.2.3.2.3. 高度な技術的対策が必要な事象

### 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's diary



#### 13.1. ■緊急相談対応



#### 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's diary



##### 13.1.1.1. ○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

### 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)

●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。

#### 13.1.2.1. ○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。

### 13.1.3. ●情報セキュリティに関する基礎知識 - CyberSec's diary



#### 13.1.3.1. ○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

#### 13.1.3.2.

#### 13.1.3.3. ○10大脅威2016【IPA】



#### 13.1.3.3.1. 10大脅威2016簡易説明資料（総合編）(PDF形式 6.02MB)



### 13.1.3.3.2. ⑦立場ごとのTop5を抜粋した簡易説明資料

#### ⑦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)

#### 13.1.3.3.2.1. ⑦10大脅威2016簡易説明資料(個人編)(PDF形式 4.79MB)

#### 13.1.3.3.2.2. ⑦10大脅威2016簡易説明資料(組織編)(PDF形式 4.67MB)

### 13.1.3.3.3. ⑦【参考】

#### 13.1.3.3.4. ⑦詳細資料：情報セキュリティ10大脅威 2016(PDF形式 3.95MB)

#### 13.1.3.3.5. ⑦2アップ印刷用(用紙1枚に2ページ分を印刷)はこちら

### 13.1.3.4. ⑧情報セキュリティ対策9カ条【NISC,IPA】(pdf形式)

#### ⑧情報セキュリティ対策9カ条【NISC,IPA】(pdf形式)

⑧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。

#### 13.1.3.4.1. ⑧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。

### 13.1.4. ●情報セキュリティ緊急対応ガイド– CyberSec’s diary

#### ●情報セキュリティ緊急対応ガイド– CyberSec’s diary

●緊急対応の段階と、情報セキュリティ対策の基本要件

#### 13.1.4.1. ●緊急対応の段階と、情報セキュリティ対策の基本要件

## 13.2. ■中小企業経営者向け情報



### 13.2.1. ●情報セキュリティ対策9カ条【NISC,IPA】(pdf形式)

#### ●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。

13.2.1.1. ○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。

### 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】

#### ●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。

13.2.2.1. ○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。

### 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)

#### ●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、従業員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。

13.2.3.1. ○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、従業員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。

#### 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ー一覧【IPA】

##### ●中小企業のためのセキュリティツールライブラリー一覧【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。

13.2.4.1. ○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。

#### 13.2.5. ●その他の各種情報へのリンク

##### ●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's diary

13.2.5.1. ○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's diary

### 13.3. ■家庭・個人向け情報

・【準備中】

## ■家庭・個人向け情報

### 13.3.1. •【準備中】

## 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

### ■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's diary (準備中)

#### 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's diary (準備中)

## 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

### ■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's diary

#### 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's diary

## 13.6. ■人材育成・人材確保

### ■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's diary

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

#### 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's diary

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

## 13.7. ■参考情報



### 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's diary



#### 13.7.1.1. ○公的機関、教育機関向け、個人ユーザー向け、事業者向け

### 13.7.2. ●情報セキュリティ関連法規リスト（更新中） - CyberSec's diary

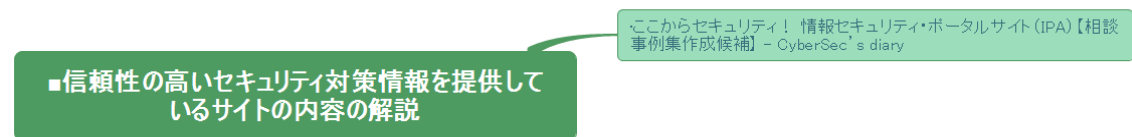
### 13.7.3. ●政府機関の情報セキュリティ対策のための統一基準群（平成26年度版） - CyberSec's diary

## 13.8. ■関連ニュース

## 13.9. ————— 相談対応の手引き用 —————



### 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



#### 13.9.1.1. ●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）【相談事例集作成候補】 - CyberSec's diary

・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's 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、  
また必要に応じて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

13.9.1.1.1. 「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、また必要に応じて内容の解説を加えたもの。

13.9.1.1.2. 検索の際はWebブラウザの検索機能を利用してください

## 13.9.2. ■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's diary

### ■事例等の紹介

13.9.2.1. ・セキュリティ侵害事例紹介サイト (FAQ候補) - CyberSec's diary

## 13.9.3. ■対策まとめ資料

### ■対策まとめ資料

・情報セキュリティ対策とは

・システム調達におけるセキュリティ要件定義

・中小企業向け対策

### 13.9.3.1. ・情報セキュリティ対策とは

・情報セキュリティポリシー、実施手順 - CyberSec's diary

・情報セキュリティに関する基礎知識 - CyberSec's diary

#### ・情報セキュリティ対策とは

・情報セキュリティ対策の概念 - CyberSec's 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's diary

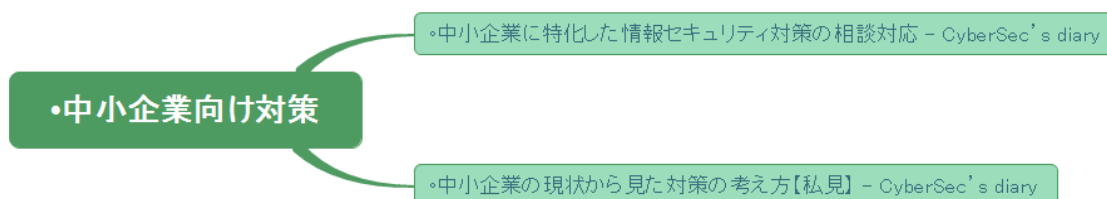
13.9.3.1.1. 情報セキュリティに関する基礎知識 - CyberSec's diary

13.9.3.1.2. ◦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's diary

13.9.3.1.3. ◦情報セキュリティ対策の概念 - CyberSec's diary

13.9.3.1.4. ◦情報セキュリティポリシー、実施手順 - CyberSec's diary

### 13.9.3.2. •中小企業向け対策



13.9.3.2.1. ◦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's diary

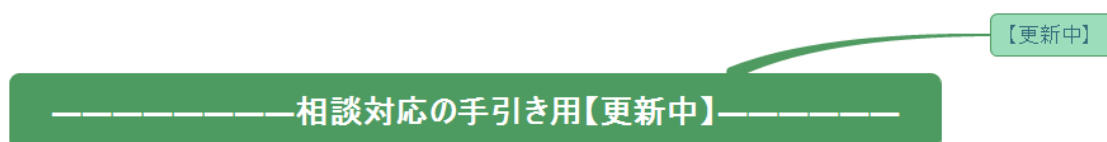
13.9.3.2.2. ◦中小企業の現状から見た対策の考え方【私見】 - CyberSec's diary

### 13.9.3.3. •システム調達におけるセキュリティ要件定義

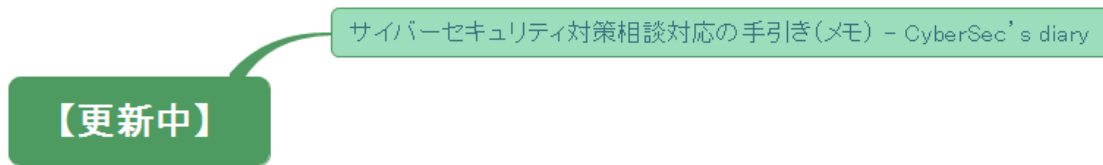


13.9.3.3.1. ◦情報システムの整備と運用管理を調達する際の情報セキュリティ対策要件（メモ） - CyberSec's diary

## 13.10. -----相談対応の手引き用【更新中】-----

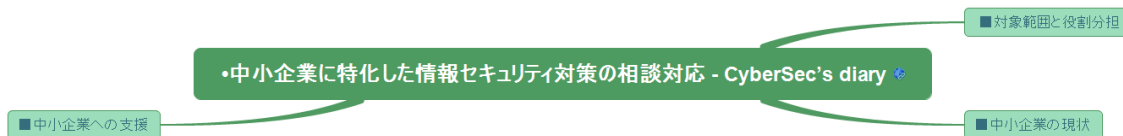


### 13.10.1. 【更新中】



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

### 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's diary](#)

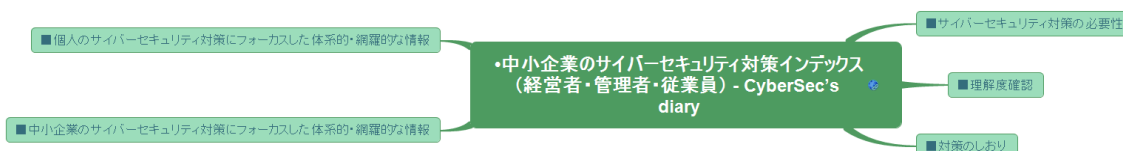


#### 14.1. ■対象範囲と役割分担

#### 14.2. ■中小企業の現状

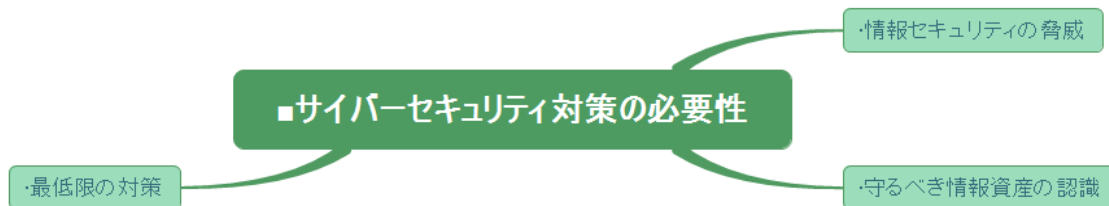
#### 14.3. ■中小企業への支援

### 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's diary](#)



#### 15.1. ■サイバーセキュリティ対策の必要性





#### 15.1.1. ●情報セキュリティの脅威

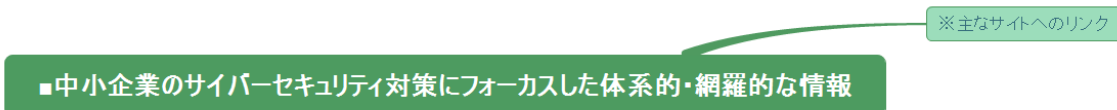
#### 15.1.2. ●守るべき情報資産の認識

#### 15.1.3. ●最低限の対策

### 15.2. ■理解度確認

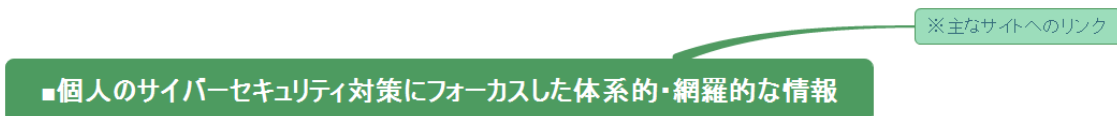
### 15.3. ■対策のしおり

### 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



#### 15.4.1. ※主なサイトへのリンク

### 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



#### 15.5.1. ※主なサイトへのリンク

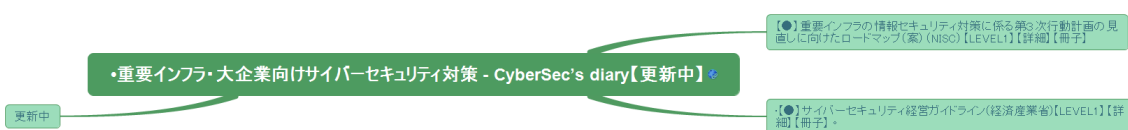
## 16. [●家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec's diary【更新中】](#)

更新中

●家庭個人向け最低限のサイバーセキュリティ対策 - CyberSec's diary【更新中】

### 16.1. 更新中

## 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's diary【更新中】](#)



### 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)【LEVEL1】【詳細】【冊子】

【●】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)【LEVEL1】【詳細】【冊子】

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

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

### 17.2. ●【●】サイバーセキュリティ経営ガイドライン(経済産業省)【LEVEL1】【詳細】【冊子】。

【●】サイバーセキュリティ経営ガイドライン(経済産業省)【LEVEL1】【詳細】【冊子】。

<http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>

<http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf>

#### 17.2.1. <http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html>

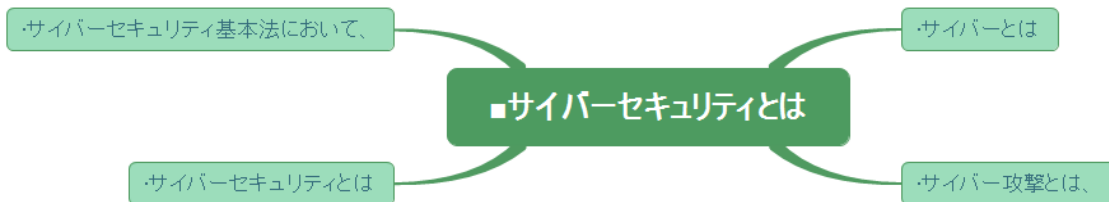
17.2.2. <http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf>

17.3. 更新中

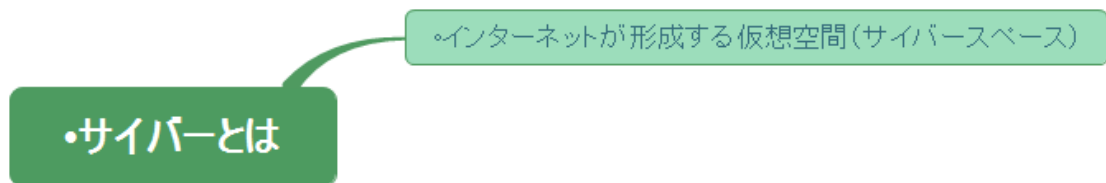
## 18. [●サイバーセキュリティとは - CyberSec's diary](#)



### 18.1. ■サイバーセキュリティとは

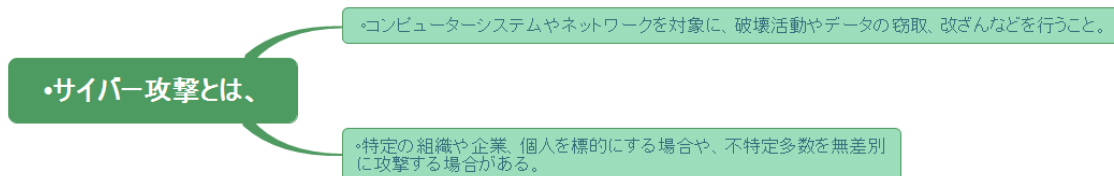


#### 18.1.1. ●サイバーとは



##### 18.1.1.1. インターネットが形成する仮想空間 (サイバースペース)

#### 18.1.2. ●サイバー攻撃とは、



#### 18.1.2.1.

◦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。

18.1.2.2. ◦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。

#### 18.1.3. •サイバーセキュリティとは

##### •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。

#### 18.1.3.1.

◦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。

#### 18.1.4. •サイバーセキュリティ基本法において、

##### •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。

#### 18.1.4.1.

◦電子的方式、磁気的方式その他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。

## 19. ●情報セキュリティに関する基礎知識 - CyberSec's diary



### 19.1. 1.1. 情報セキュリティ対策の基本

### 19.2. 1.2. 【対策】情報セキュリティ 10 大脅威 (個人)

### 19.3. 1.3. 【対策】情報セキュリティ 10 大脅威 (組織)

### 19.4. 1.4. 【対策】注目すべき脅威や懸念

### 19.5. 1.5 サービス提供と情報セキュリティ対策

## 20. ●情報セキュリティ対策の概念 - CyberSec's diary



### 20.1. 1.1. リスクの要因

### 20.2. 1.2. 情報セキュリティにおけるさまざまな対策

### 20.3. 1.3. 情報セキュリティ対策の意義

### 20.4. 1.4. 情報セキュリティ対策のポイント (私見)

## 21. ●情報セキュリティポリシー、実施手順 - CyberSec's diary



### 21.1. 1.1. 情報セキュリティポリシーの構成

### 21.2. 1.2. 情報セキュリティポリシー（基本方針）

### 21.3. 1.3. 情報セキュリティポリシー（対策基準）

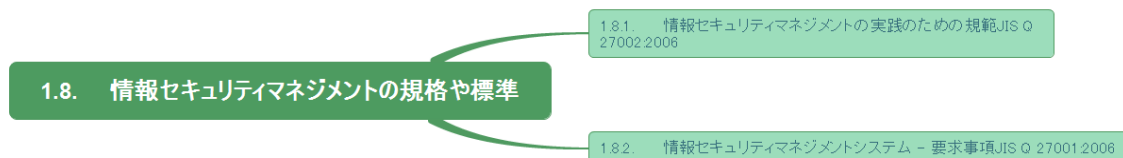
### 21.4. 1.4. 情報セキュリティ実施手順

### 21.5. 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

### 21.6. 1.6. ISMSとPDCAサイクル

### 21.7. 1.7. 脅威・対策・脆弱性・リスクの関係

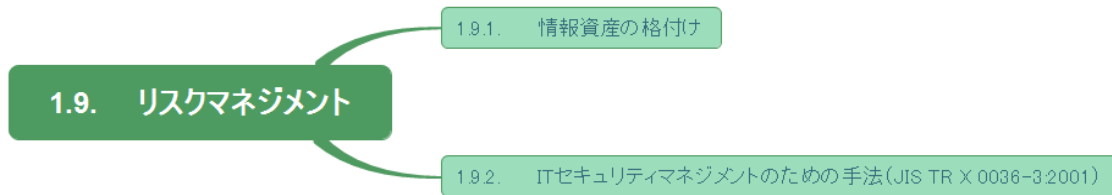
### 21.8. 1.8. 情報セキュリティマネジメントの規格や標準



#### 21.8.1. 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

#### 21.8.2. 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

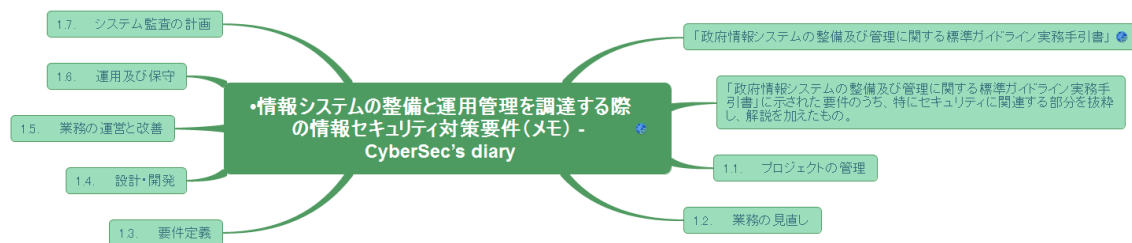
### 21.9. 1.9. リスクマネジメント



21.9.1. 1.9.1. 情報資産の格付け

21.9.2. 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)

## 22. 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's diary



### 22.1. 「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」

22.2. 「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。

22.3. 1.1. プロジェクトの管理

22.4. 1.2. 業務の見直し

22.5. 1.3. 要件定義

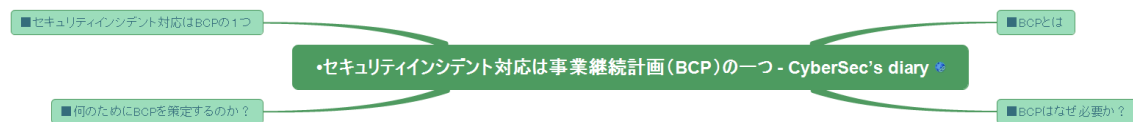
22.6. 1.4. 設計・開発

22.7. 1.5. 業務の運営と改善

22.8. 1.6. 運用及び保守

22.9. 1.7. システム監査の計画

## 23. ●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's diary



23.1. ■BCPとは

23.2. ■BCPはなぜ必要か？

23.3. ■何のためにBCPを策定するのか？

23.4. ■セキュリティインシデント対応はBCPの1つ

## 24. ●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's diary



24.1. 1.1. ITパスポート試験シラバス

24.2. 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

24.3. 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

24.4. 1.4. 情報セキュリティマネジメント試験 シラバス



24.5. 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

24.6. 1.6. 情報セキュリティ人材の職種

25. [●情報セキュリティマネジメントに必要な知識 - CyberSec's diary](#)

26. [●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's diary](#)



26.1. ○公的機関、教育機関向け、個人ユーザー向け、事業者向け

26.2. 「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。

26.3. ●公的機関

26.4. ●教育機関向け

26.5. ●個人ユーザー向け

26.6. ●事業者向け

27. [●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's diary](#)



## 27.1. ※全体的内容、規定の趣旨、対策例

## 28. ●情報セキュリティ関連法規リスト（更新中） - CyberSec's diary



### 28.1. 1.1. サイバーセキュリティ基本法

### 28.2. 1.2. 不正アクセス禁止法

### 28.3. 1.3. 個人情報保護法

### 28.4. 1.4. 刑法

### 28.5. 1.5. その他のセキュリティ関連法規

### 28.6. 1.6. 知的財産権

### 28.7. 1.7. 労働関連・取引関連法規

### 28.8. 1.8. その他の法律・ガイドライン・技術者倫理

## 29. ●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's diary



### 29.1. ●関連サイト [内閣サイバーセキュリティセンター]

### 29.2. ●関連リンク：IPA 独立行政法人 情報処理推進機構

**29.3. 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）**

**29.4. サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））**

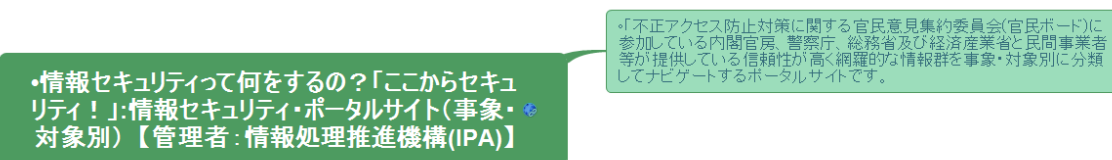
**29.5. 東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss: Tokyo Cyber Security Support network for small and medium enterprises）**

**30. 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's diary**



**30.1. 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）】**



**30.1.1.**。「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。

**30.2. 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）】**

・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)】

・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います。

30.2.1. ◦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います。

30.3. ・国民のための情報セキュリティサイト【総務省】

・国民のための情報セキュリティサイト【総務省】

・インターネットと情報セキュリティの知識の習得に役立ち、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。

30.3.1. ◦インターネットと情報セキュリティの知識の習得に役立ち、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。

30.4. ・情報セキュリティ広場【警視庁】

・情報セキュリティ広場【警視庁】

・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。

30.4.1. ◦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。

30.5. [●IS702【トレンドマイクロ】](#)

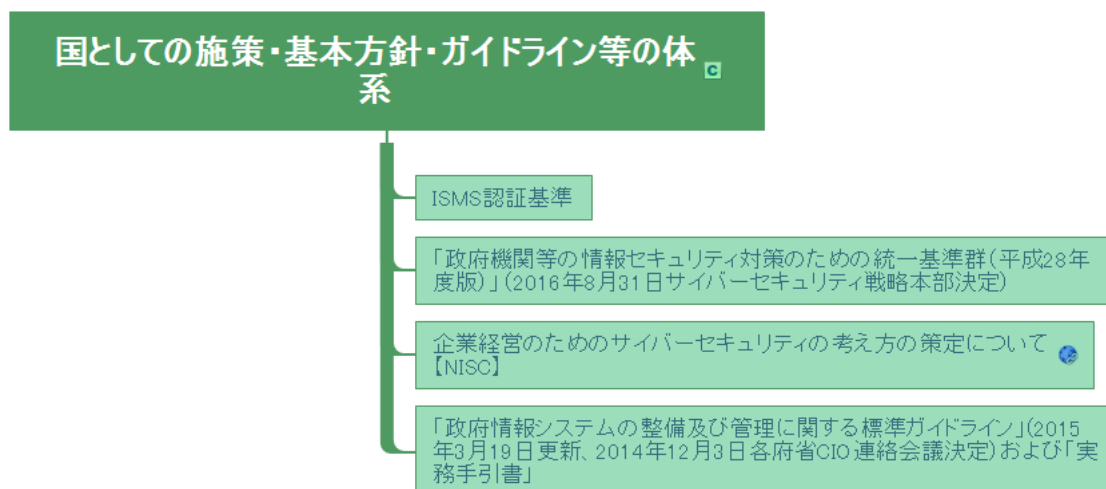
30.6. [●Security & Trust :](#)

[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】](#)

31. [●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】](#)

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

33. [国としての施策・基本方針・ガイドライン等の体系](#)



33.1. ISMS認証基準



### 33.1.1. JIS Q 27000 : 2014



#### 33.1.1.1. 情報セキュリティマネジメントシステム用語



##### 33.1.1.1.1. 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

### 33.1.2. JIS Q 27001:2014



#### 33.1.2.1. ISMS適合性評価制度における認証基準



##### 33.1.2.1.1. ISMS認証に関するガイド類

## ISMS認証に関するガイド類

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

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

33.1.3. JIS Q 27002 : 2014

## JIS Q 27002 : 2014

情報セキュリティ管理策の実践のための規範

33.1.3.1. 情報セキュリティ管理策の実践のための規範

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ー最良の慣行）をまとめた規格

33.1.3.1.1. 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ー最良の慣行）をまとめた規格

33.1.4. 【参考】

地方公共団体と情報セキュリティ（2016年3月8日JIPDEC）

## 【参考】

33.1.4.1. 地方公共団体と情報セキュリティ（2016年3月8日JIPDEC）

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

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

33.1.4.1.2. 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

33.2. 「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）

「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>

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

33.3. [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】](#)



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

33.3.2. [サイバーセキュリティ戦略本部](#)

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

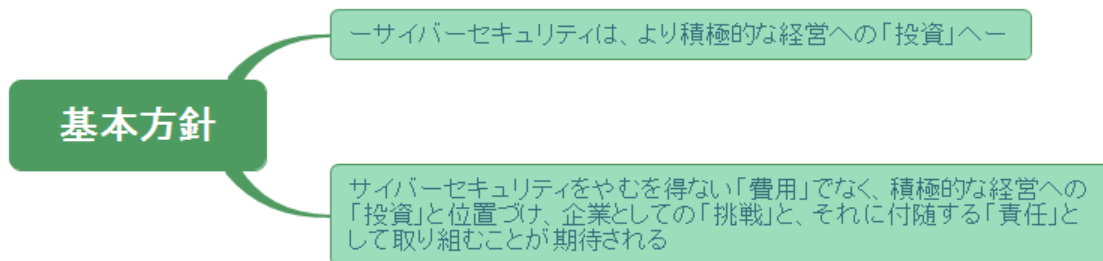
サイバーセキュリティ戦略本部



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

33.3.3. 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

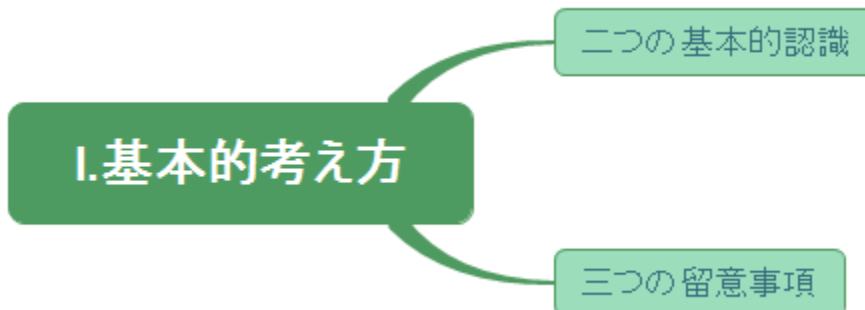
#### 33.3.4. 基本方針



33.3.4.1. 一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

33.3.4.2. 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

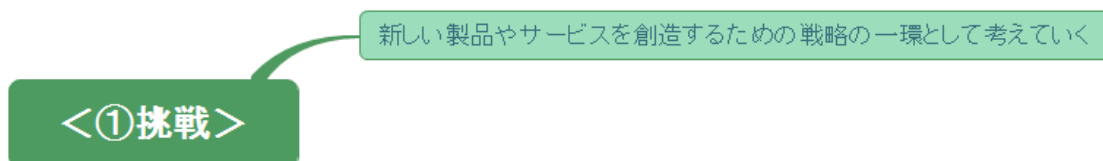
#### 33.3.5. I.基本的考え方



33.3.5.1. 二つの基本的認識

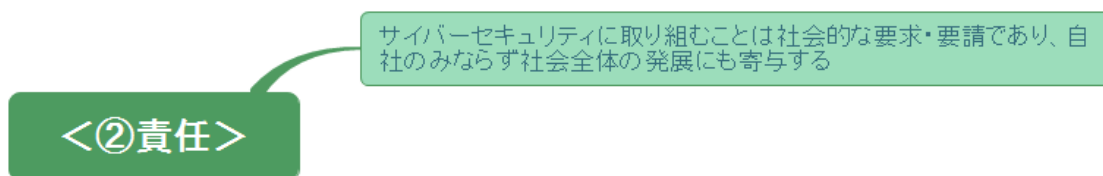


#### 33.3.5.1.1. <①挑戦>



33.3.5.1.1.1. 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

#### 33.3.5.1.2. <②責任>

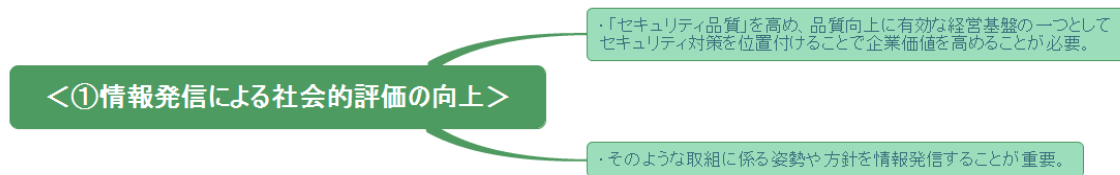


33.3.5.1.2.1. サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与する

#### 33.3.5.2. 三つの留意事項



#### 33.3.5.2.1. <①情報発信による社会的評価の向上>



##### 33.3.5.2.1.1. •

「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。

##### 33.3.5.2.1.2. •

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。

#### 33.3.5.2.2. <②リスクの一項目としてのサイバーセキュリティ>

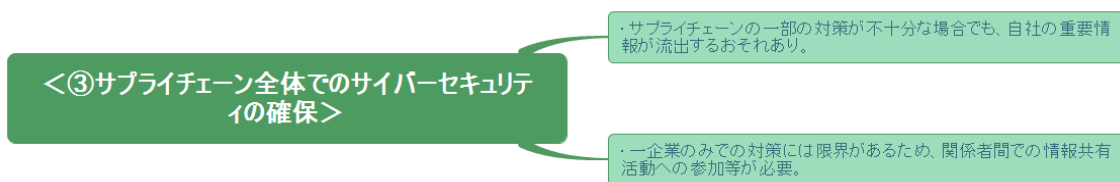


##### 33.3.5.2.2.1. •

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。

##### 33.3.5.2.2.2. • 経営層のリーダーシップが必要。

#### 33.3.5.2.3. <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>



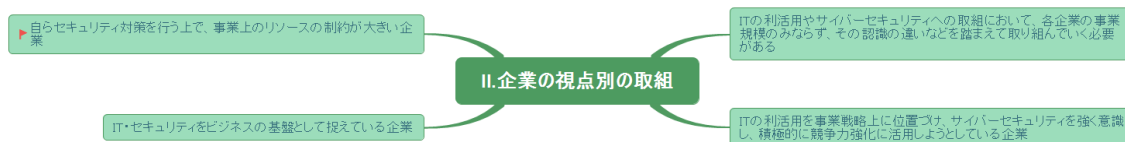
#### 33.3.5.2.3.1. •

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。

#### 33.3.5.2.3.2. •

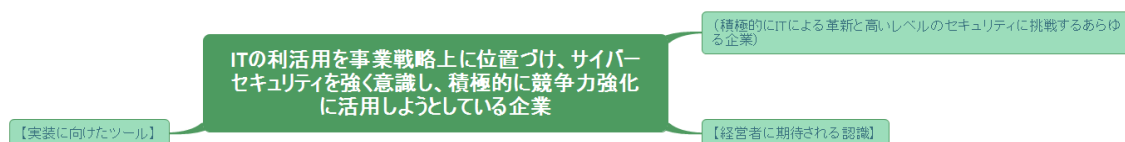
一企業のみでの対策には限界があるため、関係者間での情報共有活動への参加等が必要。

### 33.3.6. II.企業の視点別の取組



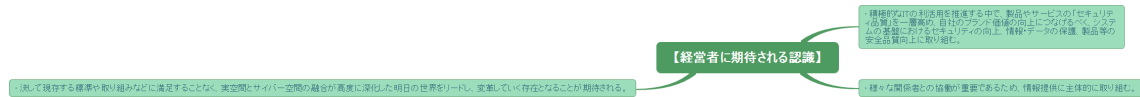
33.3.6.1. ITの利活用やサイバーセキュリティへの取組において、各企業の事業規模のみならず、その認識の違いなどを踏まえて取り組んでいく必要がある

33.3.6.2. 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



33.3.6.2.1. （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）

33.3.6.2.2. 【経営者に期待される認識】



#### 33.3.6.2.2.1. •

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。

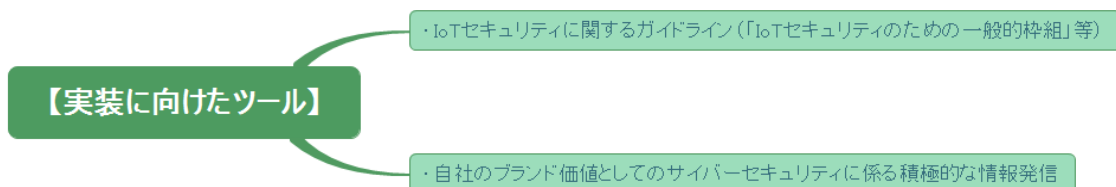
#### 33.3.6.2.2.2. •

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。

#### 33.3.6.2.2.3. •

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。

### 33.3.6.2.3. 【実装に向けたツール】



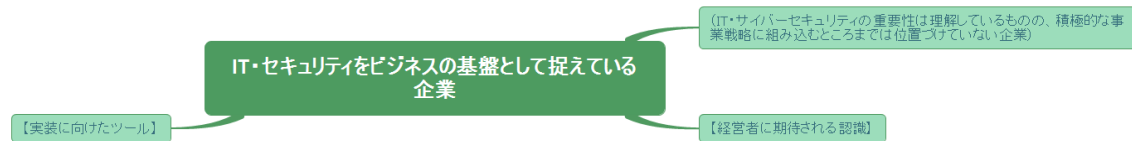
#### 33.3.6.2.3.1. •

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）

#### 33.3.6.2.3.2. •

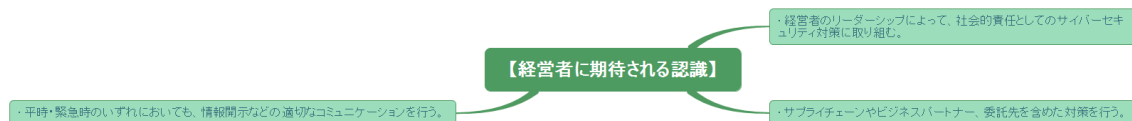
自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

### 33.3.6.3. 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



#### 33.3.6.3.1. (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)

#### 33.3.6.3.2. 【経営者に期待される認識】



##### 33.3.6.3.2.1. •

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。

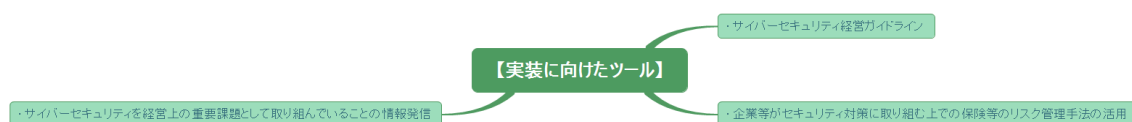
##### 33.3.6.3.2.2. •

サブ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。

##### 33.3.6.3.2.3. •

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。

#### 33.3.6.3.3. 【実装に向けたツール】



##### 33.3.6.3.3.1. • サイバーセキュリティ経営ガイドライン

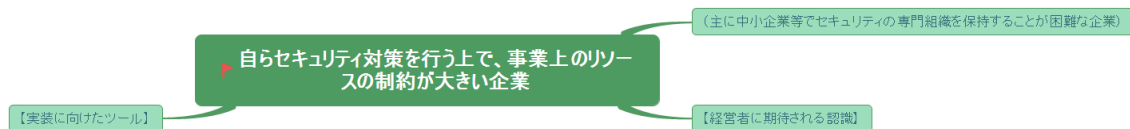
#### 33.3.6.3.3.2. •

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

#### 33.3.6.3.3.3. •

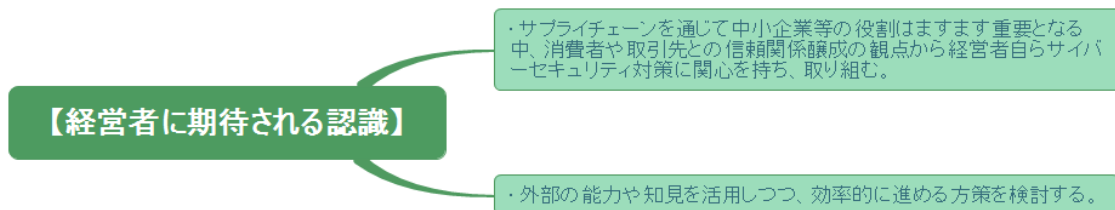
サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

### 33.3.6.4. 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



#### 33.3.6.4.1. （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）

#### 33.3.6.4.2. 【経営者に期待される認識】



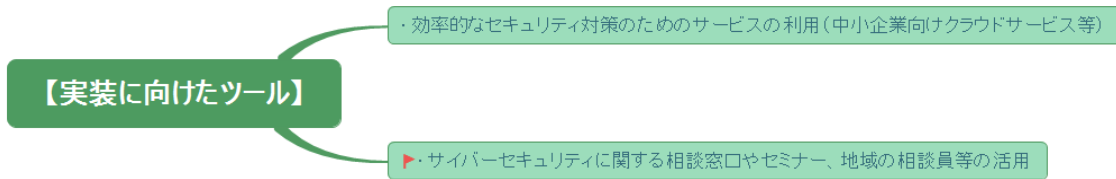
#### 33.3.6.4.2.1. •

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。

#### 33.3.6.4.2.2. •

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。

#### 33.3.6.4.3. 【実装に向けたツール】



#### 33.3.6.4.3.1. •

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）

#### 33.3.6.4.3.2. •

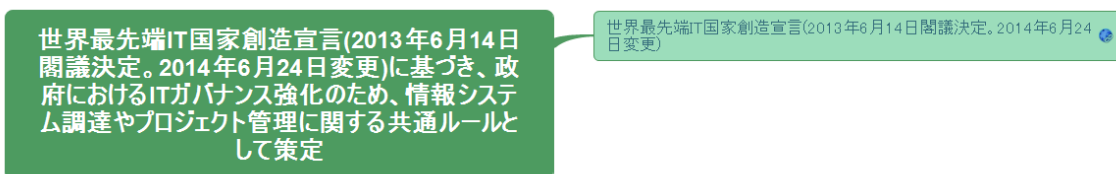
サイバーセキュリティに関する相談窓口やセミナー、地域の相談員等の活用

### 33.4. 「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」



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

#### 33.4.2. 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





**33.4.2.1. 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)**