【別紙】サイバーセキュリティに関するKPIの例

2019年4月　初版　JCIC作成

	管理番号	大項目	中項目	小項目	KPIの目安	対象組織	分類	KPI算出方法	目的／期待する効果	参考情報	URL
1	1.1.1	セキュリティ部門の施策	情報資産棚卸進捗率	ハードウェア資産棚卸進捗率	95%以上	成熟度「低」（初期段階）	組織・プロセス	棚卸を実施した情報資産数 ÷ 対象とする情報資産数	脆弱性対応などが短時間で可能となり、リスクを軽減できる	棚卸方法には「各部門からの申告ベース」と「IT資産管理ツールによる自動収集」の2種類がある。	
2	1.1.2			ソフトウェア資産棚卸進捗率	95%以上	成熟度「低」（初期段階）	組織・プロセス				
3	1.1.3			モバイル機器棚卸進捗率	95%以上	成熟度「低」（初期段階）	組織・プロセス				
4	1.1.4			利用しているクラウドサービス棚卸進捗率	90%以上	成熟度「中」（改善段階）	組織・プロセス				
5	1.2.1		法規制やガイドラインの準拠率	法規制準拠率	100%	成熟度「低」（初期段階）	法令順守	現在の実績値 ÷ 計画値	対外的な説明責任を果たし、行政指導や罰金のリスクを軽減する	日本のサイバーセキュリティや個人情報保護に関わる主な法制度には、「サイバーセキュリティ基本法」、「個人情報保護法」、「割賦販売法」、「不正アクセス禁止法」、「不正競争防止法」、「電子署名法」、「著作権法」、「刑法」、「迷惑メール防止法」などがある。 国内のガイドラインには「サイバーセキュリティ経営ガイドライン」、「個人情報の保護に関するガイドライン」などがあり、海外では「NIST Cyber Security Framework」、「情報セキュリティマネジメントシステム（ISMS）」、「SANS 20 Critical Controls」などがある。	JCIC「諸外国のサイバーセキュリティ・個人情報保護に関する法制度」 https://www.j-cic.com/column/Cybersecurity-Privacy-Law.html
6	1.2.2			個人情報の匿名化、非保持化の進捗率	100%	成熟度「中」（改善段階）	法令順守	現在の実績値 ÷ 計画値	対外的な説明責任を果たし、行政指導や罰金のリスクを軽減する	各国のプライバシー法規制に準じ、個人情報の匿名化、非保持化などの対応が必要となる。また、クレジットカード情報を保有している場合、「割賦販売法」や「PCI DSS」に準じたクレジットカード情報の匿名化、非保持化が必要となる。	
7	1.3.1		監督官庁の指摘事項対応完了率	監督官庁の指摘事項対応完了率	100%	成熟度「低」（初期段階）	法令順守	対応完了数 ÷ 指摘事項数	監督官庁への説明責任を果たし、ビジネス影響を回避	特に、重要インフラ事業者に関しては、監督官庁と内閣サイバーセキュリティセンター（NISC）の両方の指摘事項に対応することに留意すること。	
8	1.4.1		セキュリティ部門人員数	セキュリティ部門人員数	対IT人員の5%以上 対全社員数の0.25%以上	成熟度「中」（改善段階）	組織・プロセス	セキュリティ人員 ÷ IT人員 セキュリティ人員 ÷ 全社員数	スキルを有する人員を確保し、施策実行を確実にする	【カーネギーメロン大学の調査（年商60億円以上、4ヵ国の555組織が対象）】 - IT部門社員数の割合に対するセキュリティ社員は「平均5.2%」 【韓国の電子金融監督規定では、韓国金融委員会（FSC）が金融機関が最低限守るべき数値を規定】 - 全社員数に対するセキュリティ社員は「0.25%以上」（従業員1万人の場合、25人以上を確保しなければならない） - IT担当者に対するセキュリティ担当者数は「5%以上」	Carnegie Mellon University Software Engineering Institute「Structuring the Chief Information Security Officer Organization」 https://resources.sei.cmu.edu/asset_files/TechnicalNote/2015_004_001_446198.pdf 韓国電子金融監督規定 http://www.law.go.kr/행정규칙/전자금융감독규정（韓国語）, https://www.fsc.go.kr/downManager?bbsid=BBS0085&no=115218（英語抄訳版）
9	1.4.2			資格取得者数	自社の現状に合わせて設定	成熟度「中」（改善段階）	組織・プロセス	資格取得者数		情報処理安全確保支援士、CISSP（セキュリティプロフェッショナル認定資格制度）などがある。	
10	1.5.1		セキュリティ予算	対IT予算比率	対IT予算の7%以上	成熟度「中」（改善段階）	組織・プロセス	セキュリティ予算 ÷ IT予算	適切な予算を確保し、施策実行を確実にする	【カーネギーメロン大学の調査（年商60億円以上、4ヵ国の555組織が対象）】 - IT予算に対するセキュリティ予算は「平均5.1%」 【韓国の電子金融監督規定では、韓国金融委員会（FSC）が金融機関が最低限守るべき数値を規定】 - ITセキュリティ予算は、IT予算総額のうち「7%以上」（人件費、福利厚生費、研修費用、システム購入費用、保守費用等が対象）	
11	1.5.2			予算消化率	95%以上	成熟度「中」（改善段階）	組織・プロセス	使用額 ÷ 予算額			
12	1.6.1		新規システム開発の評価回数、合格率	新規システム開発の評価回数	自社の現状に合わせて設定	成熟度「中」（改善段階）	組織・プロセス	システム評価回数	セキュアなシステム構築が可能となる	NIST SP 800-64「システム開発ライフサイクルにおけるセキュリティの考慮事項」などを参照	NIST「システム開発ライフサイクルにおけるセキュリティの考慮事項（SP 800-64）」https://csrc.nist.gov/publications/detail/sp/800-64/rev-
13	1.6.2			新規システム開発の評価合格率	90%以上	成熟度「中」（改善段階）	組織・プロセス	合格数 ÷ システム評価回数			
14	1.7.1		ベンチマーク評価	ベンチマーク評価	自社の現状に合わせて設定	成熟度「中」（改善段階）	評価・アセスメント	ベンチマーク評価結果	自社の弱いポイントを客観的に把握でき、対策を具体化できる	国内のベンチマークツールには「IPA 情報セキュリティ対策ベンチマーク」、「NIRセキュア Secure SketCH」などがあり、海外では「NIST Cyber Security Framework」、「FFIEC CAT（金融機関向け）」などがある。	IPA「情報セキュリティ対策ベンチマーク」 https://www.ipa.go.jp/security/benchmark/ NIRセキュア「Secure SketCH」https://www.secure-sketch.com/ ISF「The ISF Benchmark」https://www.securityforum.org/tool/the-isf-benchmark-and-benchmark-as-a-service/ FFIEC 「Cybersecurity Assessment Tool（CAT）」 https://www.ffiec.gov/cyberassessmenttool.htm
15	1.8.1		アセスメント結果	自社のアセスメント結果		成熟度「中」（改善段階）	評価・アセスメント	アセスメント・監査結果	自社の弱いポイントを客観的に把握でき、対策を具体化できる	アセスメントや監査の方法には「インタビュー、質問表形式」と「自動化ツール」の2種類がある。自動化ツールには、「BitSight」、「SecurityScorecard」、「Cyence」、「PivotPoint Risk Analytics」などがある。	
16	1.8.2			子会社や海外現地法人のアセスメント結果		成熟度「高」（最適化段階）	評価・アセスメント	アセスメント・監査結果	ガバナンスを効かせにくいグループ子会社や海外現地法人の弱いポイントを客観的に把握でき、対策を具体化できる		
17	1.9.1		海外現地法人のガバナンス構築進捗率	全社ポリシー準拠率		成熟度「中」（改善段階）	組織・プロセス	現在の実績値 ÷ 計画値	組織全体のセキュリティレベル向上に繋がる	本社で策定したポリシーに従い、海外現地法人に対するガバナンス体制構築を実施。JCICのインタビューの中では、「中央集権的にするのか、現地にある程度の裁量を持たせるのかを最初に決めることが重要」、「3か月ごとなど定期的に直接コミュニケーションを取ることが重要」という声があった。	
18	1.9.2			監視システム導入率		成熟度「中」（改善段階）	組織・プロセス				
19	1.10.1		サイバー演習実施回数	経営層向けサイバー演習実施回数		成熟度「高」（最適化段階）	教育・トレーニング	現在の実績値 ÷ 計画値	サイバー攻撃を受けた後の被害を最小限にする	組織内のインシデント対応チーム「CSIRT（シーサート）」を中心にサイバー演習の企画・実行・振り返りを行う。公的機関などが提供する集合型のサイバー演習、自組織内で行う独自のサイバー演習の2種類がある。	JPCERT/CC「CSIRTマテリアル」 http://www.jpcert.or.jp/csirt_material/
20	1.10.2			CSIRT向けサイバー演習実施回数		成熟度「中」（改善段階）	教育・トレーニング				
21	1.10.3			グループ会社向けサイバー演習実施回数		成熟度「中」（改善段階）	教育・トレーニング				
22	1.11.1		インシデント対応完了	インシデント発見までの平均時間		成熟度「高」（最適化段階）	組織・プロセス	不正侵入から検知までの平均時間	潜伏期間を短くすることで被害を軽減	MTTI: Mean Time To Identify（情報漏えいが発生したことを検出するまでにかかった時間の平均）という用語を用いることがある	Ponemon Institute社/IBM社「2018 Cost of Data Breach Study」 https://www.ibm.com/security/data-breach
23	1.11.2			インシデント対応完了平均時間・工数		成熟度「高」（最適化段階）	組織・プロセス	検知から封じ込めまでの平均時間	短時間に封じ込めることで、被害を最小限にする	MTTC: Mean Time To Contain（情報漏えいを食い止めるまでにかかった時間の平均）という用語を用いることがある。	
24	1.12.1		脆弱性対応	脆弱性対応着手までの平均時間		成熟度「高」（最適化段階）	組織・プロセス	緊急な脆弱性の公開から着手までの平均時間	緊急度の高い脆弱性をすぐに着手することでリスクを軽減	自社システムに影響のある脆弱性について、脆弱性CVSS共通脆弱性評価システムを用いて、自社システム環境を考慮した評価を行う前提。	「CVSS共通脆弱性評価システム」 https://jvndb.jvn.jp/cvss/ja/v3.html
25	1.12.2			脆弱性対応完了までの平均時間・工数		成熟度「高」（最適化段階）	組織・プロセス	着手から対応完了までの平均時間	緊急度の高い脆弱性をすぐに対応することでリスクを回避	更なる対策強化のため、脆弱性通報プログラムなどにより、積極的に脆弱性情報を収集する仕組み作りも検討する必要がある。	
26	1.13.1		業界内の情報共有体制構築	迅速にインシデント情報を入手するための業界内体制構築	業界の現状に合わせて設定	成熟度「高」（最適化段階）	業界内の情報共有・連携	現在の実績値 ÷ 計画値	自社だけで得られない情報を得ることで対策強化できる	日本国内では、サイバー情報共有イニシアティブ（J-CSIP）、日本シーサート協議会、業界毎のISAC（情報共有分析組織）などがある。	
27	1.13.2			業界ガイドラインの策定		成熟度「高」（最適化段階）	業界内の情報共有・連携	現在の実績値 ÷ 計画値			
28	2.1.1	経営層の巻き込み	経営層打合せ回数	経営層打合せ回数	自社の現状に合わせて設定	成熟度「中」（改善段階）	組織・プロセス	打合せ回数	経営層の理解を促進し、サイバーセキュリティ対策推進をサポートしてもらえる	特に、経営戦略改定があった場合、異動や組織変更があった場合などに経営層打合せを実施する。	
29	2.1.2			役員会議・経営会議出席回数		成熟度「高」（最適化段階）	組織・プロセス	出席回数			
30	3.1.1	自社システム	標準システムポリシー準拠率	ハードニング対応率	95%以上	成熟度「中」（改善段階）	組織・プロセス	対応完了数 ÷ 対象システム数	会社で定めたセキュリティ対策を実施することにより、全社的なセキュリティレベルを向上できる	標準システムポリシーを策定する場合、対象となるシステムを特定することが前提となる。定期的に準拠状況を把握する必要がある。	
31	3.1.2			特権アカウント管理の対応率	95%以上	成熟度「中」（改善段階）	組織・プロセス				
32	3.1.3			BCP策定完了率	95%以上	成熟度「中」（改善段階）	組織・プロセス				
33	4.2.1	社員教育	セキュリティ教育受講率	受講率	95%以上	成熟度「低」（初期段階）	教育・トレーニング	受講者数 ÷ 教育対象者数	社員の意識啓発を促進し、全社的なセキュリティレベルを向上できる	教育対象者は、全社員を対象にするのか、派遣社員や業務委託者も対象にするのかをあらかじめ決める必要がある。また、受講率だけではなく、テストの合格率も把握する必要がある。	
34	4.2.2			テスト合格率	85%以上	成熟度「中」（改善段階）	教育・トレーニング	テスト合格者数 ÷ 受講者数			
35	4.3.1		標的型メール訓練開封率	標的型メール訓練実施回数	自社の現状に合わせて設定	成熟度「低」（初期段階）	教育・トレーニング	実施回数	標的型メールに対する意識を向上させ、怪しい添付ファイルなどは開かないこと、開いた場合は適切な対処を行うことができる	昨今の標的型メール訓練は、開封率だけを把握するだけでは十分ではなく、開封した者に対する再訓練や追加トレーニングなども実施することが重視されている。	
36	4.3.2			再テスト開封率	自社の現状に合わせて設定	成熟度「中」（改善段階）	教育・トレーニング	開封者数 ÷ 訓練対象者数			
37	4.3.3			開封者に対するトレーニング受講率	90%以上	成熟度「中」（改善段階）	教育・トレーニング	受講者数 ÷ 開封者数			
38	5.1.1	取引先・サプライチェーンの監査	外部委託監査進捗率	外部委託監査進捗率	自社の現状に合わせて設定	成熟度「中」（改善段階）	評価・アセスメント	監査実施数 ÷ 監査対象	取引先・サプライチェーンからの情報流出などを防ぐことができる	取引先との契約内容に基づき、「インタビュー」、「現地調査」、「質問表形式」などの手法で監査を定期的に実施することが望ましい。	
39	5.1.2			指摘事項対応率		成熟度「中」（改善段階）	評価・アセスメント	指摘事項完了数 ÷ 指摘事項数			
40	5.2.1		M&A、提携先の評価回数	M&A、提携先の評価回数		成熟度「高」（最適化段階）	評価・アセスメント	評価回数	M&A、提携先のセキュリティ評価を行うことで、ビジネスリスクを軽減できる	デューデリジェンス（相手先の価値やリスクなどの調査）の一環でサイバーセキュリティ状況を把握することが望ましい。	
41	6.1.1	プロジェクト	事故対応手順の策定	事故対応手順の承認	計画値に対して遅延がないこと	成熟度「低」（初期段階）	組織・プロセス	現在の実績値 ÷ 計画値	プロジェクトを計画通りに進めることで、着実に組織全体のセキュリティレベル向上を図る	プロジェクト計画時に、作業スケジュールを詳細化したWBS（Work Breakdown Structure）を作成し、実績値と計画値を定期的に把握することが必要。	
42	6.1.2			全社展開進捗率		成熟度「中」（改善段階）	組織・プロセス				
43	6.2.1		公表判定基準の策定	公表判定基準の承認		成熟度「中」（改善段階）	組織・プロセス				
44	6.2.2			全社展開進捗率		成熟度「高」（最適化段階）	組織・プロセス				
45	6.3.1		新セキュリティシステム導入進捗率	新セキュリティシステム導入進捗率		成熟度「中」（改善段階）	組織・プロセス				
46	6.3.2			プロジェクトレビュー数		成熟度「中」（改善段階）	組織・プロセス				
47	6.4.1		新法規制対応進捗率	新法規制対応進捗率		成熟度「中」（改善段階）	法令順守				