参考資料　サイバーリスクに関するKRIの例

2019年10月　初版　JCIC作成

管理番号	大項目	中項目	小項目	KRI上限値（しきい値）の目安	期待する効果	参考情報	URL
1.1.1	組織外の動向 （海外・国内動向）	サイバー攻撃の検知・防御件数	標的型メール攻撃件数（警察庁）	3か月前より件数が1.5倍以上 （公的機関が定点観測している統計レポートをもとに総合的にリスク度を算出。例えば、標的型攻撃メール件数や不正アクセス件数が3か月前より1.5倍以上となったら高リスクとする）	世の中のサイバーリスクの差し迫り度合いを客観的に把握することができる	定点観測レポートは過去から現在の脅威を把握するための統計情報として利用することができる。	警察庁「サイバー空間に関する統計等」https://www.npa.go.jp/publications/statistics/cybersecurity/index.html IPA「J-CSIP運用状況」https://www.ipa.go.jp/security/J-CSIP/index.html IPA「コンピュータウイルス・不正アクセスの届出状況および相談状況」https://www.ipa.go.jp/security/txt/2018/q2outline.html JPCERT/CC「インターネット定点観測レポート」http://www.jpcert.or.jp/tsubame/report/index.html フィッシング対策協議会「月次報告書」http://www.antiphishing.jp/report/monthly/
1.1.2			不正アクセス件数（警察庁）				
1.1.3			不正送金件数（警察庁）				
1.1.4			不正送金被害額（警察庁）				
1.1.5			コンピュータウイルス届出状況（IPA）				
1.1.6			コンピュータ不正アクセス届出状況（IPA）				
1.1.7			フィッシング報告状況（フィッシング対策協議会）				
1.1.8			ISACからの共有件数				
1.2.1		脆弱性件数	緊急の脆弱性件数（CVSSv3基本値＝9.0～10.0）	深刻度が「緊急」と定義された脆弱性の件数が3か月前より1.5倍以上	世の中の脆弱性の深刻度や件数を客観的に把握することができる	自社システムで利用していない脆弱性も全体傾向を把握するために集計する。	IPA「JVN iPediaの登録状況」https://www.ipa.go.jp/security/vuln/index.html#section6 JPCERT/CC「Weekly Report」http://www.jpcert.or.jp/wr/2018.html US-CERT https://www.us-cert.gov/ncas/current-activity CERT-EU https://cert.europa.eu/cert/filteredition/en/VulnerabilitiesAll.html
1.2.2			重要の脆弱性件数（CVSSv3基本値＝7.0～8.9）				
1.2.3			ISACからの共有件数				
2.1.1	組織内の傾向 （自社・グループ会社の傾向）	インシデント件数	重大インシデント件数	重大インシデント件数（2件以上／3か月）	自社やグループ会社のリスク発生状況を把握し、具体的なリスク対応に繋げる	自社の各部門やグループ会社からインシデント情報が報告され、一元的に管理していることが前提となる。また、インシデントレベルの重大、中程度、軽微といったレベル設定は、社内の情報セキュリティ規程類などにしたがって定義する。	
2.1.2			中インシデント件数				
2.1.3			軽微インシデント件数				
2.2.1		サイバー攻撃の検知・防御件数	ファイアウォール防御数	3か月前より2倍以上	自社に対するリスクの差し迫り度合を客観的に把握することができる	事前に、自社に対する攻撃シナリオを洗い出し、どのログを集計するべきかを把握していることが前提となる。	
2.2.2			マルウェア検知数				
2.2.3			不正ログイン試行数				
2.3.1		インシデントによる停止時間	インシデントによる停止時間・縮退時間		システムの停止時間や縮退時間によるビジネス影響を把握することができる	インシデント起因のシステム停止、縮退稼働（片系運転）に関しての情報を把握できることが前提となる。	
2.4.1		設定ミス	本番稼働後の設定ミス件数		設定ミスによるリスクを把握することができる	システムの設定ミスに関しての情報を把握できることが前提となる。	
2.5.1		自社システムに影響のある脆弱性件数	緊急の脆弱性件数		自社で利用するシステムの脆弱性を客観的に把握することができる	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
2.5.2			重要の脆弱性件数				
2.5.3			定期的な脆弱性診断結果				
2.6.1		顧客からの問い合わせ件数	セキュリティに関する問い合わせ・クレーム件数		顧客からの声を集計することで、ビジネス影響の予兆を把握することができる	営業部門、顧客サポート部門などからセキュリティに関する問い合わせ・クレーム件数を把握する前提。	
2.7.1		第三者セキュリティチェック評価	第三者セキュリティチェック評価		自社の弱いポイントを客観的に把握できる	「BitSight」、「RiskRecon」、「Prevalent」、「SecurityScorecard」、「Cyence」、「PivotPoint Risk Analytics」などがある。	
2.8.1		外部のレピュテーション調査評価	ダークウェブの書き込み件数		サイバー攻撃の予兆、ビジネス影響の予兆を把握することができる	有償サービスの利用、自社による監視などで実現する。	
2.8.2			SNS書き込み件数				
3.1.1	取引先・サプライチェーンの傾向	インシデント件数	報告された重大セキュリティインシデント件数	重大インシデント件数（2件以上／3か月）	取引先やサプライチェーンのリスク状況を把握し、具体的なリスク対応に繋げる	取引先などからインシデント情報が自社に報告される契約になっているか、具体的な報告プロセスが構築されているかを確認することが前提となる。	
3.1.2			報告された中程度セキュリティインシデント件数				
3.2.1		監査指摘件数	取引先監査の重大指摘件数	前回監査より2倍以上		セキュリティ監査には、実地監査や調査票などの手法がある。	