2019 年 10 月

【コメンタリー】
なぜ、金融機関はサイバーリスク管理に「KRI」を用いるのか

■ サイバーリスク増大に伴い KRI を導入する金融機関

「KRI」という用語をご存知でしょうか。KRI とは、Key Risk Indicators の頭文字をとったもので、日本語では「重要リスク指標」と訳されます。**リスクを定量的にモニタリングする項目の上限値（しきい値）**を意味し、主に経営リスク管理の分野で**経営のためのツールとして用いられています。**

JCIC が国内の金融機関のセキュリティ責任者へのインタビューを行ったところ、「KRI」を用いてサイバーリスク管理を行っている事例が複数社ありました。**デジタル技術への依存度が高い金融機関では、近年サイバーリスクが経営に与える影響が大きくなってきておりますが**、なぜ、サイバーリスク管理に「KRI」を用いているのでしょうか。

本コラムでは、セキュリティ部門やリスク管理部門を想定読者とし、リスクをモニタリングする指標である KRI とは何か、どのような効果が期待できるかを説明し、日本企業への示唆を示します。

■ サイバーリスク管理のための KRI とは

まず、企業のリスク管理委員会や情報セキュリティ委員会などが、経営層へサイバーリスクを報告する例を示します。この報告例では、ヒヤリハットを含めたセキュリティ事故件数（インシデント件数）を KRI 指標としてモニタリングした結果を表しています。また、リスク度や傾向（トレンド）を図示し、リスクが顕在化した際の対応も明記しています。セキュリティ事故の重大性については、あらかじめ社内規程類などで定めてあることが前提となっています。

図表 1 サイバーリスク報告例

カテゴリ	インシデント件数	リスク状況	リスク度	トレンド	リスク対応
組織外の動向①（海外・国内動向）※	内容 / 件数（前回） 標的型メール 5,438件（2,578） 不正アクセス 2,848件/日（1780） KRI：3か月前より件数が1.5倍以上	国内で業務停止を伴うメール経由のサイバー攻撃が増加。 ②同業他社のA社にて被害が発生し、工場の操業が2日間停止。	高リスク	上昇傾向	・外部環境や取引先の状況から、リスクが拡大しているため、当社の警戒態勢を高める。 ・同業他社Aの原因調査を至急行い、当社の対策を見直す。 ・システム停止が発生した場合の業務継続計画を再点検する。
自社内・グループ会社	Level / 件数（前回） 重大（KRI） 0件（0） 中程度 5件（8） 軽微 23件（20）	重大事故は発生しなかったが、メール経由のウイルス感染が5件発生。もし、当社工場が2日間停止すると5千万円の被害。	中リスク	変化なし	
取引先・サプライチェーン③	Level / 件数（前回） 重大（KRI） 1件（0） 中程度 6件（2） 軽微 8件（5）	取引先B社がサイバー攻撃を受け、顧客情報が盗難された。当社及び当社顧客の情報は含まれていなかった。	中リスク	上昇傾向	

【インシデント件数に関するKRI】（3か月ごとに計測）
高リスク：重大インシデント件数 「2件以上」
中リスク：重大インシデント件数 「1件以下」or 中程度「5件以上」
低リスク：高・中リスク以下のもの
※組織外動向のKRIは、3か月前より件数が1.5倍以上の場合、高リスクと定義

報告例の中身を見ていくと、①「組織外の動向」で標的型メールの件数が 3 か月前に比べ 2 倍以上にもなっており、②同業他社で工場の操業が 2 日間も停止するという事態が発生しています。また、③「取引先・サプライチェーン」でも重大インシデントが 1 件発生していることがわかります。自社内・グループ会社では重大インシデントは発生していませんが、自社周辺でリスクが非常に差し迫っていることをストーリーとして語ることができ、具体的なリスク対応（リスク低減・保有・回避・移転など）が求められていることを経営層に対して強調することができます。

■ ビジネス目標に沿った KRI の設定方法

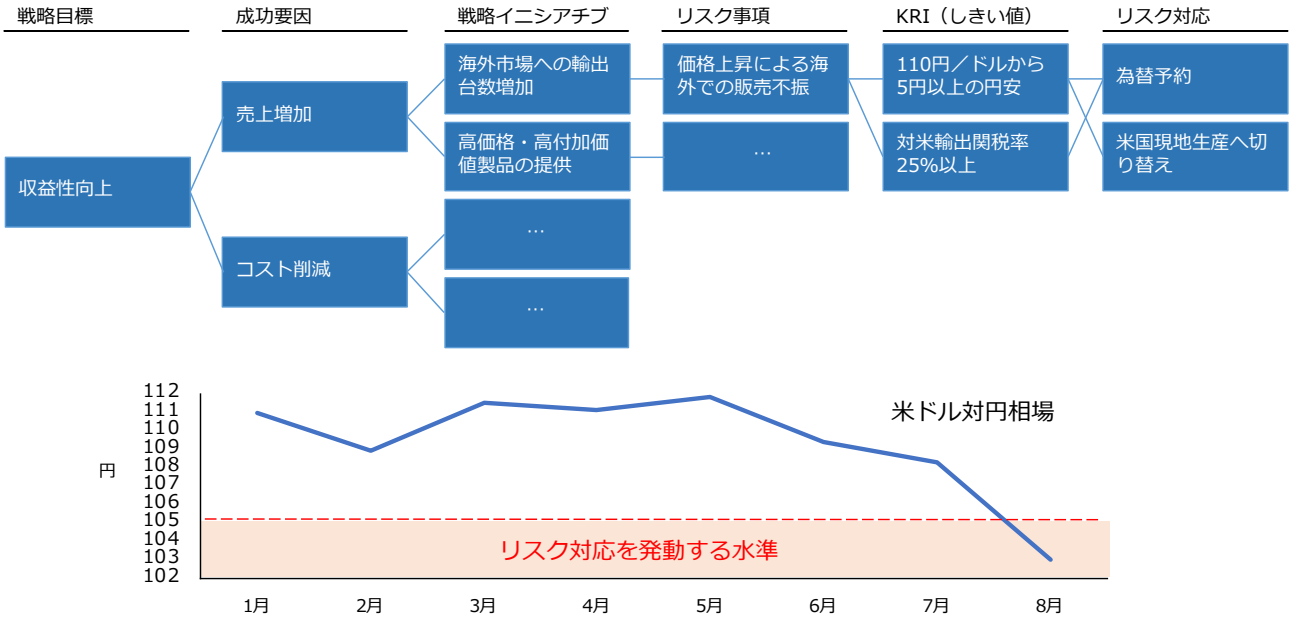
リスクをモニタリングする指標である KRI は、経営リスク管理の分野で広く活用されています。内部統制のフレームワークを開発している団体[1]は、KRI を次の通り説明しています。ある企業のビジネス目標として、「収益性（Profitability）の向上」が掲げられているとします。収益性を向上させるための成功要因を分解すると、「売上増加」と「コスト削減」に分けられます。これらを実現するために、「重要な施策（戦略イニシアチブ）」を設定します。そして、成功を妨げる「障壁（潜在リスク）」を洗い出し、リスクにつながる根本事象（リスク要因）の指標を KRI として定めます。このようなプロセスで KRI を検討すると、ビジネス目標に沿った KRI を設定でき、経営リスクを管理しやすくなります。

図表 2 ビジネス目標に沿った KRI の設定方法（COSO）

[1] COSO（米国トレッドウェイ委員会組織委員会）「Developing Key Risk Indicators to Strengthen Enterprise Risk Management」, https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf

それでは、具体なリスクシナリオの例を見ていきましょう。図表 3 の例では、「収益性向上」を目指す国内自動車部品メーカーが、「売上増加」のために「海外市場への輸出台数増加」という施策（戦略イニシアチブ）を設定し、リスク事項として「価格上昇による海外での販売不振」を掲げています。このリスクをモニタリングする KRI として、「米ドル対円相場」と「対米輸出関税率」の 2 つを設定しました。KRI には、上限値（しきい値）が必要ですが、これは公開情報を基にした数値や自社の過去データから抽出します。また、この指標を超過した場合のリスク対応（リスク低減・保有・回避・移転など）も、事前に関係者と検討し、文書化しておくと、いざという時に役に立ちます。なお、サイバーリスクに関するリスクシナリオ例を Appendix に掲載してありますので、ぜひとも参考にしてください。

図表 3 国内自動車部品メーカーのリスクシナリオの例



■ KRI 導入のメリット

サイバーセキュリティは経営課題だと言われて久しいですが、いまだに経営層と現場のギャップは埋まっていません。海外の調査によると、8 割の企業が取締役会にサイバーセキュリティに関する戦略を報告していますが、有益な報告を受け取っていると答えた取締役は 3 割弱しかいとのことです [2]。つまり、サイバーセキュリティの戦略を取締役や経営層に報告をしても、一部にしか理解されない傾向が

[2] PwC コンサルティング合同会社「Digital Trust Insights」,
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2019/assets/pdf/digitaltrustinsights.pdf

あります。自然災害などとは異なり、サイバーリスクは目に見えないため、適切に管理するためにはKRI のような「リスクの見える化（可視化）」が必要です[3]。

リスクの見える化（可視化）をするためには、リスクをモニタリングする指標である KRI を用いることが有効です。オーストラリア財務省によれば、KRI を導入することで、以下の 4 つのメリットがあるとのことです[4]。

- **リスク評価の理解促進**：KRI はリスク評価に付加情報を加えることで、経営層が自社のリスクを詳細に把握することに役立つ
- **新たなリスクの予防**：有益なフレームワークを作成することで、KRI は新たなリスクの特定を可能にする
- **上限値（しきい値）と許容レベルの設定**：KRI は経営層が注目すべき重要なレベルや直接介入すべきレベルを示す
- **KRI のトレンド把握**：KRI は経営層が自組織に対するリスクの傾向を把握することに役立つ

このように、KRI は健康診断のように、自社のサイバーリスクの見える化（可視化）が実現でき、リスクを適切に管理することに役立つことから、主に金融機関を中心に導入が広がっています。

■ KRI の具体例

それでは、企業はどのような KRI をモニタリング対象にしているのでしょうか。海外では、KRI に関する研究が数多くありますので、参考になる情報を以下に示します。

- **KRI Handbook（opsdog 社）[5]**
  情報セキュリティに関する 47 個の KRI 例、IT システムに関する 64 個の KRI 例が列挙されています。
  【KRI 例】 ログが収集できているシステムの割合、システムリリースが失敗した割合
- **Key Risk Indicator a Complete Guide（The Art of Service 社）[6]**
  KRI に関する自己診断用の質問に回答すると自社のスコアがわかります。また、プロジェクトマネージャー向けの KRI に関する質問が列挙されています。
  【質問例】KRI の責任者は特定されていますか、KRI の報告タイミングは決まっていますか

[3] 高度セキュリティ実務者向け認定資格「CompTIA Advanced Security Practitioner (CASP)」では、KRI が出題範囲に含まれる。
[4] オーストラリア政府「Understanding and developing key risk indicators」, https://www.finance.gov.au/sites/default/files/comcover-information-sheet-understanding-and-developing-key-risk-indicators.pdf
[5] opsdog 社「KRI Handbook」, https://opsdog.com/resources/key-risk-indicators-examples-kris-technology-risk-management/
[6] The Art of Service 社「Key Risk Indicator a Complete Guide」, https://theartofservice.com/

ここで、JCIC が国内の複数金融機関にヒアリングした内容をもとに、KRI として定量的にモニタリングする内容と上限値（しきい値）の目安を示します。詳細については、参考資料「サイバーリスクの KRI 例.pdf」をご覧ください。なお、過去データを収集・分析し、例えば 10 年に 1 度しか発生しないリスク事象を【高リスク】、3 年に 1 度程度発生するリスク事象を【中リスク】などと設定している事例もありました。

図表 4 サイバーリスクとしてモニタリングする項目例と KRI の上限値（しきい値）の目安

管理番号	大項目	中項目	小項目	KRI上限値（しきい値）の目安
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
4			ISACからの共有件数	
5		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
6	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）
7		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
8			マルウェア検知数	
9			不正ログイン試行数	
10		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	
11		設定ミス	本番稼働後の設定ミス件数	
12		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	
13		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	
14		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	
15		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	
16			SNS書き込み件数	
17	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）

■ KRI と KPI の違い

リスクをモニタリングする指標である「KRI」と似たような可視化や数値化の手法として、「KPI」があります[7]。KRI と KPI は、厳格な定義が存在しているわけではなく、可視化の目的や用途によって使われ方が異なります。KRI は KPI の裏返し、つまり KPI が事業目標達成度を可視化するもの、KRI はその事業目標の裏にあるリスク状況を可視化するものと考えることもできます。また、全く同じ指標でも、部門によって目線が異なるという理由から、リスク管理部門は KRI として管理し、セキュリティ部門では KPI として設定しているケースもあります（「サイバーセキュリティの KPI」については、JCIC レポート参照）[8]。

[7] 他にも、業種／企業／部門によって、KSF（重要成功要因；Key Success Factors）、KGI（重要目標指標；Key Goal Indicators）、RPI（リスク先行指標；Risk Precursory Indicators）といった可視化・数値化の指標が用いられることがあります。

[8] https://www.j-cic.com/pdf/report/KPI-Report-JA.pdf

JCIC のインタビューでは、KRI を「自組織ではコントロールできないリスク度を全社横断的に測るもの」、KPI を「自組織でコントロール可能なものであり、部門単位の施策の達成度を評価する目標や指標」として考えている企業がありました。各企業へのインタビューや文献をもとに、KRI と KPI の違いについて以下にまとめました。導入検討にあたっては、KRI はインシデント件数のしきい値とリスク対応の設定から着手すること、KPI は社員教育受講率など自組織で管理できることから着手することが現実的なアプローチです。

図表 5 KRI と KPI の活用方法の整理 [9]

	KRI（重要リスク指標） Key Risk Indicators	KPI（重要パフォーマンス指標） Key Performance Indicators
説明	経営視点でリスク度や脅威レベルを測る指標であり、自組織でコントロールできないもの	施策の達成度を評価する目標や指標であり、自組織でコントロール可能なもの
目的	経営視点で全社的リスクに対する監督を行う（第2のディフェンスラインの視点）	現場部門の業績達成状況を評価する（第1のディフェンスラインの視点）
特徴	全社横断的	部門単位、個人単位
用途	• リスク管理や経営企画部門が、全社的リスク管理で用いる（金融機関で多く用いられる） • リスクの予兆を把握し、経営判断に役立てる	• 組織単位や個人単位で、業績の達成状況を評価するために用いる • 目標の障壁となる課題を洗い出す
報告先	• 経営層 • CRO、リスク管理部門など	• 部門責任者 • CISO、CIOなど
具体例	• 物価指数 • 原油価格 • 重大インシデント件数	• プロジェクト完了率 • 社員教育受講率 • 重大インシデント対応完了までの平均時間

■ 企業内の誰が KRI をリードすべきか

多くの企業では、**「リスク管理委員会」**や**「情報セキュリティ委員会」**が存在し、複数の部署で構成されます。KRI をリードすべき組織は、これらの委員会が最も適しています。なぜならば、全社横断的にリスクを把握できること、複数部署で構成されるため他のリスクと比較しやすいこと、定期的に経営層に報告する仕組みが既に構築されているからです。このような委員会が存在しない企業では、リスク管理部門、コンプライアンス部門、セキュリティ部門といった**「第二のディフェンスライン[10]」**が KRI をリードすべきです。

なお、サイバーリスクの KRI を導入する際の失敗例を以下に示します。

- 自社の他のリスクと比較せずに、サイバーリスクの KRI だけを経営層に報告する
- 自社のリスク動向だけを経営層に報告し、世間の動向と比較しない
- モニタリングする KRI が多すぎて、どれが重要なリスクなのかわからない

[9] 各種公開情報より JCIC が作成: CRO（最高リスク管理責任者）、CISO（最高情報セキュリティ責任者）、CIO（最高情報責任者）

[10] 独立した立場でリスクに対する監視・助言を行い、またリスク管理フレームワークの設計およびその維持、改善を実施する部署を指す。 https://www.pwc.com/jp/ja/knowledge/column/viewpoint/grc-column001.html

- KRI を細かくマイクロマネジメントしすぎて、経営層が理解できず、関心が薄れる
- KRI の上限値（しきい値）を超過した際のリスク対応の責任者が明確化されていない

■ 日本企業への示唆

これまで述べてきた通り、リスクをモニタリングする指標である KRI の導入によって、経営者が自社のサイバーリスクを詳細に把握でき、将来のリスクの予防ができる効果があります。**デジタル技術への依存度が高い金融機関では、サイバーリスクが経営に与える影響が大きいこと、金融工学を用いたリスク管理が浸透していることなどが理由で、KRI の導入が進んでいると考えられます**。この理由を鑑みると、日本の**「重要インフラ事業者」**や**「デジタルトランスフォーメーションに積極的に取り組む企業」**も、KRI の導入はメリットが非常に大きいはずです。

人間の健康診断のように、KRI によって自社のサイバーリスクの見える化（可視化）を行わないと、リスクの予兆を把握することができないため、リスクが顕在した場合の対応に遅れが出てしまい、自社ビジネスに多大な影響が発生する恐れがあります。また、KRI によってリスク上限値を定量化すること、またリスク発生時の対応と責任者を明文化することで、リスク対応発動のトリガーと対応案が明確になるため、インシデントによる影響を最小化することができます。

最後に、企業内で KRI を検討する契機になりうる日本政府の取組みをご紹介します。2019 年 6 月に経済産業省が「グループ・ガバナンス・システムに関する実務指針 」を公表し、「親会社の取締役会レベルで、（中略）セキュリティ対策の在り方について検討されるべきである」と明記しました。取締役会でサイバーセキュリティをどのように議論すべきかという点は、今後 JCIC が調査する予定ですが、図表 1 のような KRI を用いてサイバーリスク状況と対応策を報告することは、リスクの全体像を把握したいと考える取締役などにとって有効な手段です。**日本企業は、トップダウンとボトムアップの両方のアプローチが適しているため、セキュリティ部門やリスク管理部門の責任者は、先んじて KRI 導入を検討することが求められます。**

図表 1 サイバーリスク報告例（再掲）

カテゴリ	インシデント件数	リスク状況	リスク度	トレンド	リスク対応
組織外の動向（海外・国内動向）※ ①	内容：標的型メール 5,438件（2,578）／不正アクセス 2,848件/日（1780） KRI：3か月前より件数が1.5倍以上	国内で業務停止を伴うメール経由のサイバー攻撃が増加。 ② 同業他社のA社にて被害が発生し、工場の操業が2日間停止。	高リスク	上昇傾向	・外部環境や取引先の状況から、リスクが拡大しているため、当社の警戒態勢を高める。 ・同業他社Aの原因調査を至急行い、当社の対策を見直す。 ・システム停止が発生した場合の業務継続計画を再点検する。
自社内・グループ会社	Level：重大（KRI） 0件（0）／中程度 5件（8）／軽微 23件（20）	重大事故は発生しなかったが、メール経由のウイルス感染が5件発生。もし、当社工場が2日間停止すると5千万円の被害。	中リスク	変化なし	
取引先・サプライチェーン ③	Level：重大（KRI） 1件（0）／中程度 6件（2）／軽微 8件（5）	取引先B社がサイバー攻撃を受け、顧客情報が盗難された。当社及び当社顧客の情報は含まれていなかった。	中リスク	上昇傾向	

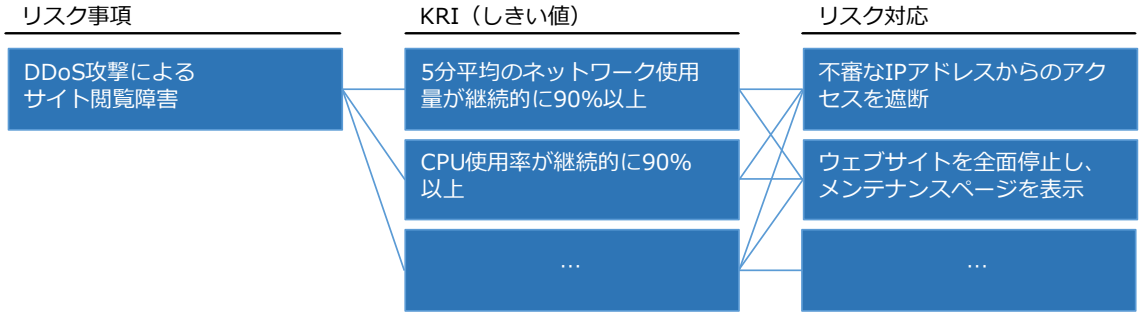
【インシデント件数に関するKRI】（3か月ごとに計測）
高リスク：重大インシデント件数 「2件以上」
中リスク：重大インシデント件数 「1件以下」or 中程度「5件以上」
低リスク：高・中リスク以下のもの
※組織外動向のKRIは、3か月前より件数が1.5倍以上の場合、高リスクと定義

以 上

（Appendix）サイバーリスクに関するリスクシナリオの例

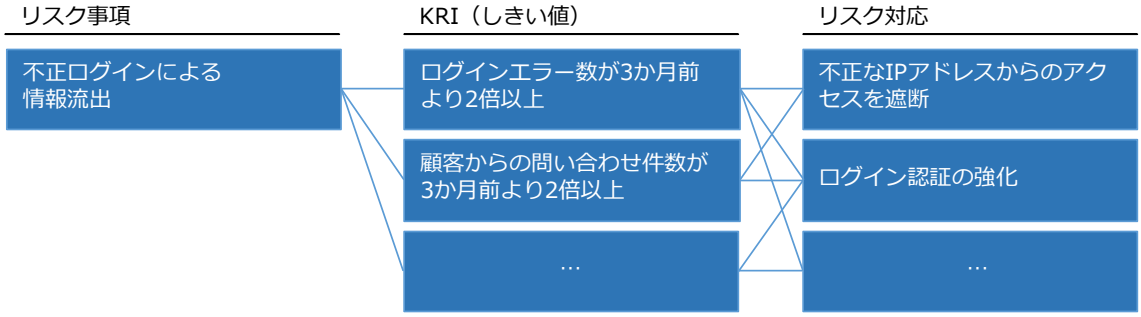
サイバーリスクに関する KRI の種類、しきい値超過時のリスク対応を具体的にイメージしていただくため、リスクシナリオ例を以下に示します。なお、企業毎に直面している事業リスクやサイバーリスクが異なるため、全ての企業で共通で用いることのできる KRI やリスク対応手法は存在しません。一般的には、リスクシナリオを検討する際は、トップダウンアプローチ（経営戦略視点）とボトムアップアプローチ（現場視点）の組み合わせで検討されます。

- ウェブサイト閲覧障害に関するリスクシナリオ

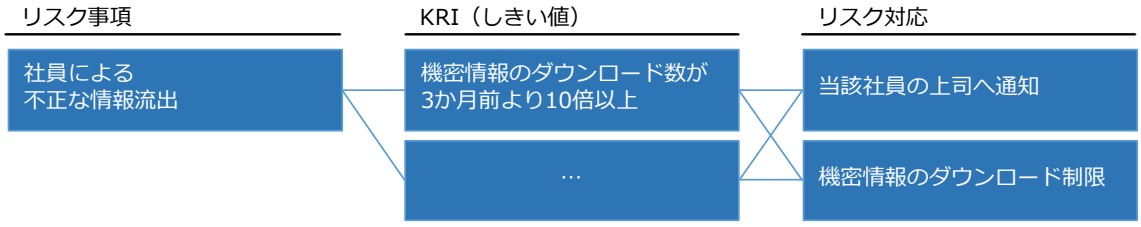


DDoS 攻撃：サービス不能攻撃のこと。世界中から高負荷をかけ、ホームページをダウンさせる攻撃

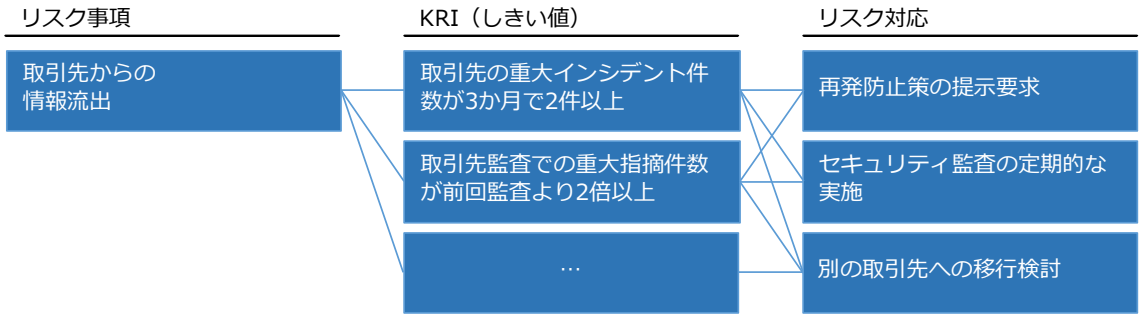
- 自社システムへの不正ログインによる情報流出に関するリスクシナリオ



- 社員による不正な情報流出に関するリスクシナリオ



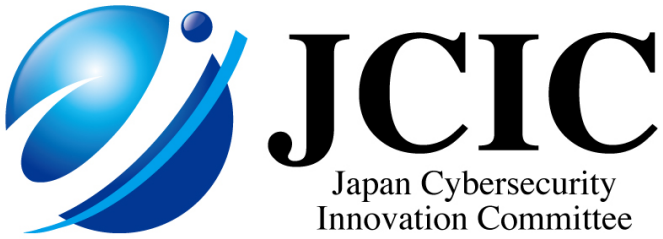
- 取引先からの不正な情報流出に関するリスクシナリオ



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。	



[本内容に関する照会先]

主任研究員　上杉謙二　uesugi@j-cic.com