

企業における SNSリスクリテラシーと対策の研究

システム監査学会

情報セキュリティ対策の診断研究プロジェクト

SNSリスクリテラシー研究会

昨年の研究から

前回大会の内容

SNSの
急速な普及で
多発する
問題発言

私的な問題に
留まらない
企業への影響

企業の
SNS管理の
責任や教育、
監査のあり方

前回の研究大会後(2012年7月11日)に、大会報告の内容を再構成した内容で、当研究メンバー以外の学会員も参加いただいてディスカッション。

ディスカッションの議題

社員の私的なSNS利用に対し、企業はどこまで責任を持つのか。

- 就業規則で定める懲戒の事由にあたる事例であり、罰則であれば十分ではないか(過失による会社への損害、素行不良で社内の秩序及び風紀を乱したとき)。
- 罰則とは別に、不適切な発言によって、誰もが被害を被るため、安易な発言によって社員を不幸にしないためにも一定の教育が必要ではないか。

SNS利用における社員のリスク領域

【 昨年2月以降にTwitter上で発生した、学生アルバイトを含む社会人の事件17件の傾向 】

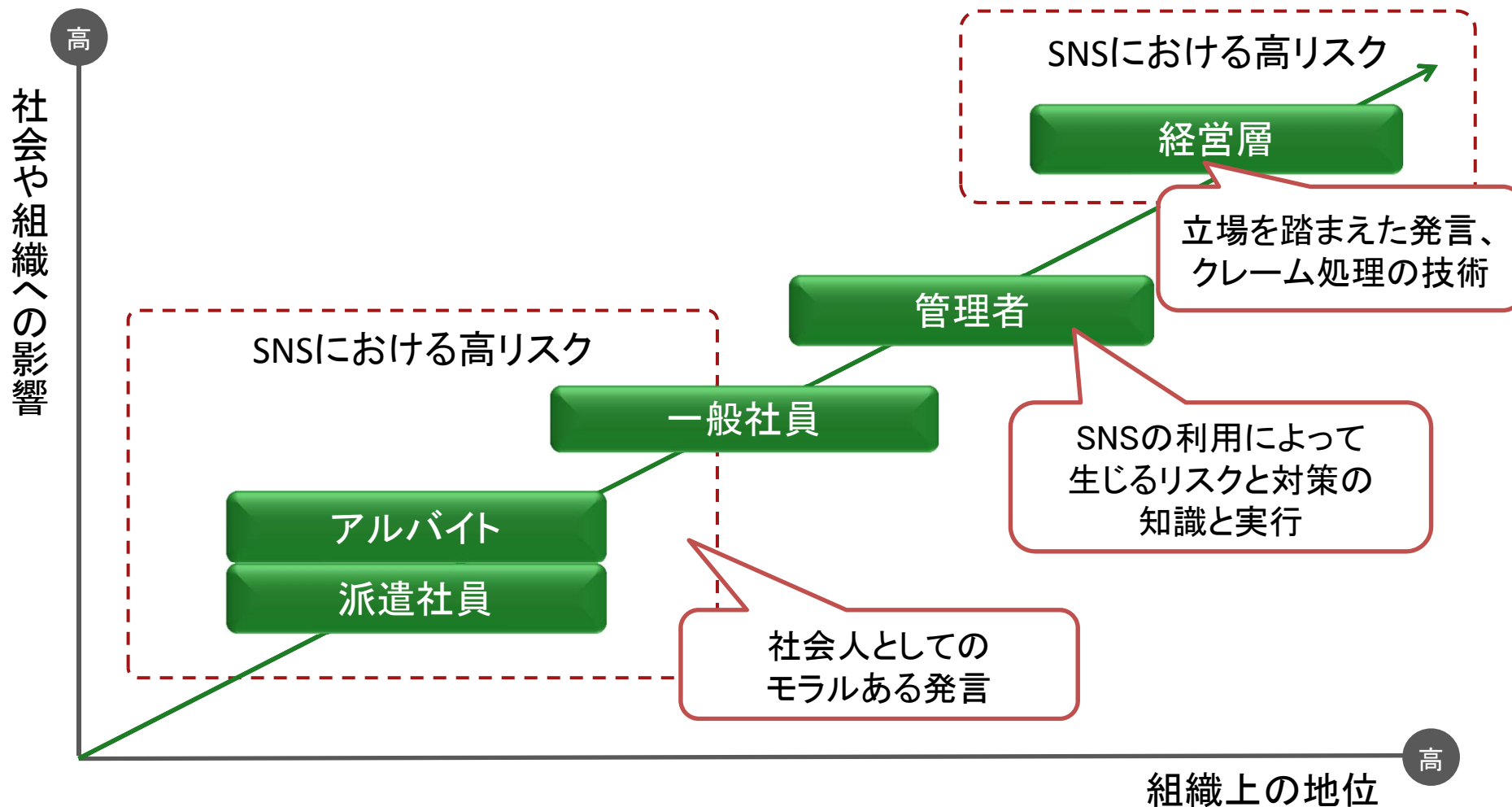
リスク発信の種類	発言する者の立場	件数	リスク領域
業務で知り得た情報を発信	社員	1件	情報セキュリティ
ユーザーとのチャットや人の意見に対する攻撃的な発言	社長や政治家など社会的地位が高い者	8件	ITリテラシー
犯罪の告白など本人のモラルに関わる発言	アルバイト、社員	8件	ITリテラシー

SNSを起因とした問題に対して

**モラル、人間性の問題として、
従来の情報セキュリティ教育でカバーしない部分が発生**

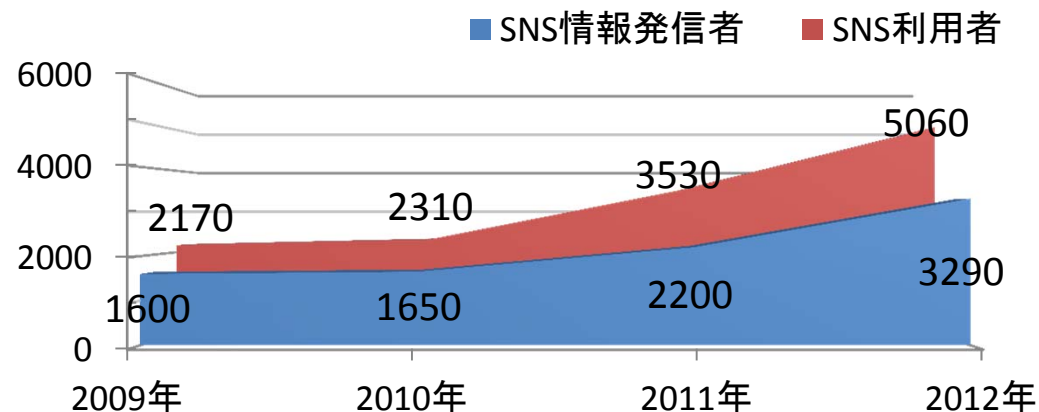
- ➡ プライベートな領域には触れない。
- ➡ モラルや一般常識は、当たり前的事として省略し、教育が不十分。

ポジションに応じて求められる対応



企業の立場で発言する者も増加

手軽に誰もが無料で参加できる
FacebookやTwitter等を中心にSNS
利用者の人口増加とともに、情報の
発信者も比例して増えている。



【インターネットメディア総合研究所「インターネット利用動向調査」より】

利用者増と比例して、
増える企業の
公式なSNSサイトの開設

公式SNSの開設によって、
増える企業のSNS担当者

企業コンプライアンスに
不十分な者が担当する機会

身近な者への発言感覚で
相手への配慮が不足

公式でありながら、
個人の立場で
意見が分かれる内容を発言

クレームの窓口として
用いられ、対応を見誤る

SNSの利用によって顕在化するリスク

従来、組織がセキュリティの対象とした情報資産は、
識別、分類により定義された情報（文書、個人データ、営業機密ファイルなど）。



個人的に見たり聞いたりした情報を、
公私を問わずに業務プロセスとかけ離れた場所で発してしまう情報

SNSの利用拡大に伴う、情報セキュリティ上の新たな対応として、次のリスクが挙げられる。

- ① 発信者本人にとっての想定外な情報拡散へのリスク
- ② 価値観の多様化された大衆への情報発信リスク
- ③ プライベートとオフィシャルのボーダレスと曖昧さ
- ④ 問題收拾への対応能力の不足でのリスク
- ⑤ これらを学習する環境が整備されていないリスク(学校教育レベル、社会人教育レベル)

SNSリスクリテラシーチェックリストの作成

従業員のSNS知識レベルを知るために「企業のSNSリスクリテラシーチェックリスト」を作成

“SNSリスクリテラシー”を定義

企業の従業員に求められるSNS利用のための基本的な知識・能力。

この能力を従業員が備えているか？

発言の善悪、影響を判断できる力

誤解のない表現で発言する力

STEP1

炎上事例を参考に「SNSリスクリテラシーチェックリスト」を作成 (2012年9月)

STEP2

SNSリスクリテラシー状況把握のため企業診断を実施 (2012年10月～2013年1月)

< 企業におけるSNS利用状況、利用する従業員のリテラシー状況はどうか >

STEP3

「SNSリスクリテラシーチェックリスト」の見直し (2013年2月～)

< 診断に値する内容が得られたか >

SNSリスクリテラシーチェックリストの内容

カテゴリ	チェックする項目(サンプル)1項目に月、約10ほどの質問を用意
① 利用状況について	<ul style="list-style-type: none"> • 発言したいと思ったら、すぐに発言していますか。 • あなたは、直接、会ったことのない人からの友達申請を承諾したことがありますか。ある場合、どの様な理由から承諾しましたか。
② サービスの理解	<ul style="list-style-type: none"> • SNSが用意する設定内容について、確認したり、設定を変更した上で使用していますか。 • SNSが用意した利用規約を読んだことはありますか。
③ 発言内容	<ul style="list-style-type: none"> • あなたがSNS上で発言した内容を読むことができるのは誰か、その公開範囲を理解していますか。 • 仕事に関連した発言をするときは、それが会社の秘密に関わらないように意識していますか。
④ 身元判明の認識	<ul style="list-style-type: none"> • GPS機能の付いたデジカメやスマートフォンで自宅を撮影した写真をアップロードする際、GPS情報の付加について毎回、確認していますか。 • あなたは、自分の氏名をインターネット上で検索し、どの様な検索結果が表示されるか、確認したことがありますか。
⑤ SNS利用の企業タスク	<ul style="list-style-type: none"> • 企業として活用するSNSは、その目的や役割、位置づけを明確にしていますか。 • SNSの担当者が発言する内容の基準やテーマなどを決め、またNGワードなど、発言してはならない用語等を決めていますか。

〔参考〕 SNSリスクリテラシーチェック診断方法(基本の考え)

1. 診断適用基準

(1)「SNSリスクリテラシーチェックリスト」(*)に基づいて実施

* : 情報セキュリティ対策診断研究プロジェクト SNS診断研究会チーム (2012.11.12版)
(SNSに関わる事故事例及び想定リスクに基づき作成したチェックリスト)

(2) チェック項目(前ページにある①-⑤の項目に分類): 「企業利用として」、「個人利用として」に分けて適用

- ① SNSの利用状況について: SNSというサービスを認識し、どのように利用しているか。
- ② SNSのサービスについて: SNS利用のルールを認識して、遵守している程度を測る。
- ③ SNSにおける発言内容: 発言内容により発生するリスクの認識の程度。
- ④ SNSを通じて身元が判明するリスクの認識: SNSの利用環境および発言が他人により使われる際に発生するリスク。
- ⑤ SNSを利用している企業のタスク(対象者の所属企業について): 企業として必要となるSNS利用のリスク対策への対応度合を測る。

2. チェックリストにより現状を調査

- SNSの利用に関して従業員の状況、業務の実態を把握する(レベル1-5)に位置づける)
- レベル: 前々年まで研究の成熟度モデルを参考(レベル1(初期/その場対応)、レベル5(最適化できている))

3. 対象企業のあるべき姿の調査

- (1) 対象企業のSNS利用に関して業務の実態、従業員のあるべき姿を把握・検討(レベル1-5)に位置づける)
- (2) その位置づけと、現状を比較し評価する

4. 結果 : 比較し評価に差がある場合にその差を解消するべく、何をするのが必要か、明確にする。

5. 改善方法の提案(具体的展開)

: チェック項目分野に関して、“定着させる形態”、“推奨案”を提示する。

〔参考〕 診断例の紹介

診断例

S社 業種 情報サービス業 (対象部署: SNSアプリケーション開発組織、一般社員組織)

1. 診断目的

企業の業務活動に悪影響を与えることがないように、組織または社員によるSNSの利用において、必要なリテラシーを持っているか。社員のSNS利用に関して企業が対処すべきことを認識し、実施しているか。それらのルールの制定状況と周知状況をチェックする。今後のSNS利用に関しての提案を行う。

2. 総評

- ① 非公式なSNS取り組みルールにより(試験的に)運営されている
利用に必要なルールを作るというよりは、発生する問題について、都度適切な判断を関係者、リーダーが行っていく。問題は発生していない。
次の状況にあることから見てうなずける状況である。
 - 業務分野として取り組み始めたばかり
 - SNS利用業務の売上げに占める割合は1割ほどで、担当者も少ない
 - これまで取り組んできた業務分野とは異なる分野で、SNSに関連する情報発信、取得情報および技術分野の蓄積は少ない
- ② あるべき姿
現状は、SNSの利用状況から見て合理的な範囲。ただし、この分野は「これから進めていく分野であり、進めていく方向にある」という。従って、現状では大きな問題はないが、今後に向けて積極的な対処をすることが望まれる。
⇒ 次(あるべき姿の検討)への対応が望ましい。

3. あるべき状況

貴社はARアプリの商品化を手がかりにSNS分野での業務を広げていくことを考えている。
今後は企業として、次を目指すことを目標とすべきと考える。

- 直接SNS関連業務に関わる社員(SNSを利用する)に関してはレベル3
- 直接SNSを業務として利用しない社員の個人利用に関してはレベル2以上

4. 診断結果 分野別に(「企業利用として」、「個人利用として」に分けて)数値評価

5. 改善提案 SNS(に直接関わる、直接関わらないに分けて)分野別に提案

- ① SNSを企業の事業として取り組む姿勢をポリシーや標準として打ち出し、教育を通じて従業員にリスク認識を持たせる
- ② 企業としてのSNS利用に関する提案

SNSリスクリテラシーの向上の施策

診断に用いた「SNSリスクリテラシーチェックリスト」のリスク分類の課題

「SNSリスクリテラシーチェックリスト」は、研究会で2012年に起きた企業が被害を受けた、情報漏えいを中心とする事件・事故の事例を元に作成。

一般的な企業の従業員のリスクリテラシー教育のベースにしてよいか

- ILASのリスク分類によるインターネットリスクの見直し

(Internet Literacy Assessment indicator for Students)

ILAS(青少年のインターネット・リテラシーに関する指標)において体系化されたリスク分類があり、社会人に対する指標としても参考になる。

- ILASから、企業関係者向けに活用できる内容を選択する

- 従業員への周知・徹底教育の内容の見直しに利用する
- 「SNSリスクリテラシー」の診断内容も検討

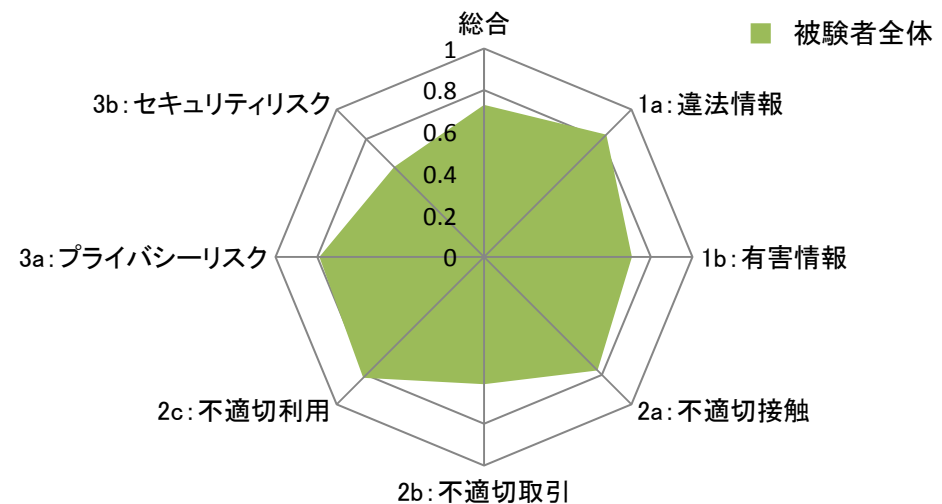
(Internet Literacy Assessment indicator for **businessman** としての検討)

ILASを用いる意義

- ILASは、インターネットリテラシーを指標化するための評価方法、テスト問題のセットで構成されているため、リテラシー教育の学習効果を評価できる（下記画像は実践例）
- ILASを元にしたインターネットリテラシーの資格制度「デジタルコンテンツアセッサ(DCA)」が、一般社団法人インターネットコンテンツ審査監視機構により開始されている（同資格の認定講座を、青山学院大、東京工科大、千葉商科大、東北福祉大、埼玉工業大で開講準備中）。
- ILASのリスク体系は、OECDによるインターネットのリスク体系を元にしてしている（資料2）。このリスク体系は、汎用性があり青少年に限定されるものではない。
- よって、ILASの基本的なリスク体系を利用しつつ、中小企業の従業員に要求されるSNSリスクリテラシーに拡張することで、汎用性のある評価が期待できる。

【 リスク中分類毎の正答率 】

総合	0.73
1a:違法情報	0.83
1b:有害情報	0.71
2a:不適切接触	0.77
2b:不適切取引	0.61
2c:不適切利用	0.82
3a:プライバシーリスク	0.79
3b:セキュリティリスク	0.61



〔 ILASの公表 (www.soumu.go.jp/menu_news/s-news/01kiban08_02000092.html) 〕

今後の展開

今後展開される新評価制度としての監査のフィールド調査研究テーマ

1 SNS情報への 監査アプローチ

- 組織の目的と過去の事件事例を考慮したSNS利用のガイドラインの制定
- 関係者全てへのSNS利用のリテラシー（作法）教育の徹底状況
- ガイドラインに沿った行動（SNS内の検索ワードの検討）
- トラブル／炎上発生時の事業継続計画の実効性の検証

2 SNSに関わる 公開情報への 監査アプローチ

- ステルスマーケティング
- ニュースリリース等の配信管理
- Twitter等の発言内容（インターネット選挙運動による想定リスクも視野に）

3 SNS利用の リスクリテラシー へのアプローチ

- BYOD（Bring Your Own Device,私的デバイス活用）
（スマートフォン、タブレット端末など）
- ILASを参考に、見直したチェックリストを用いて、
企業リスクリテラシーの向上施策を検討

謝辞 メンバー募集 など

一緒に研究する方を募集しています。

当研究プロジェクトでは、ほぼ毎月1回の研究会を開催しています。

場所

東京都南部労政会館 会議室(山手線大崎駅から5分)

時期・時間

毎月中旬、水曜(原則)の18:30から約2時間

研究結果については、HPに公表します。

さらに詳細は、当研究プロジェクト(学会事務局経由)まで

<問い合わせの窓口アドレス>

<http://www.sysaudit.gr.jp/toiawase/index.html>

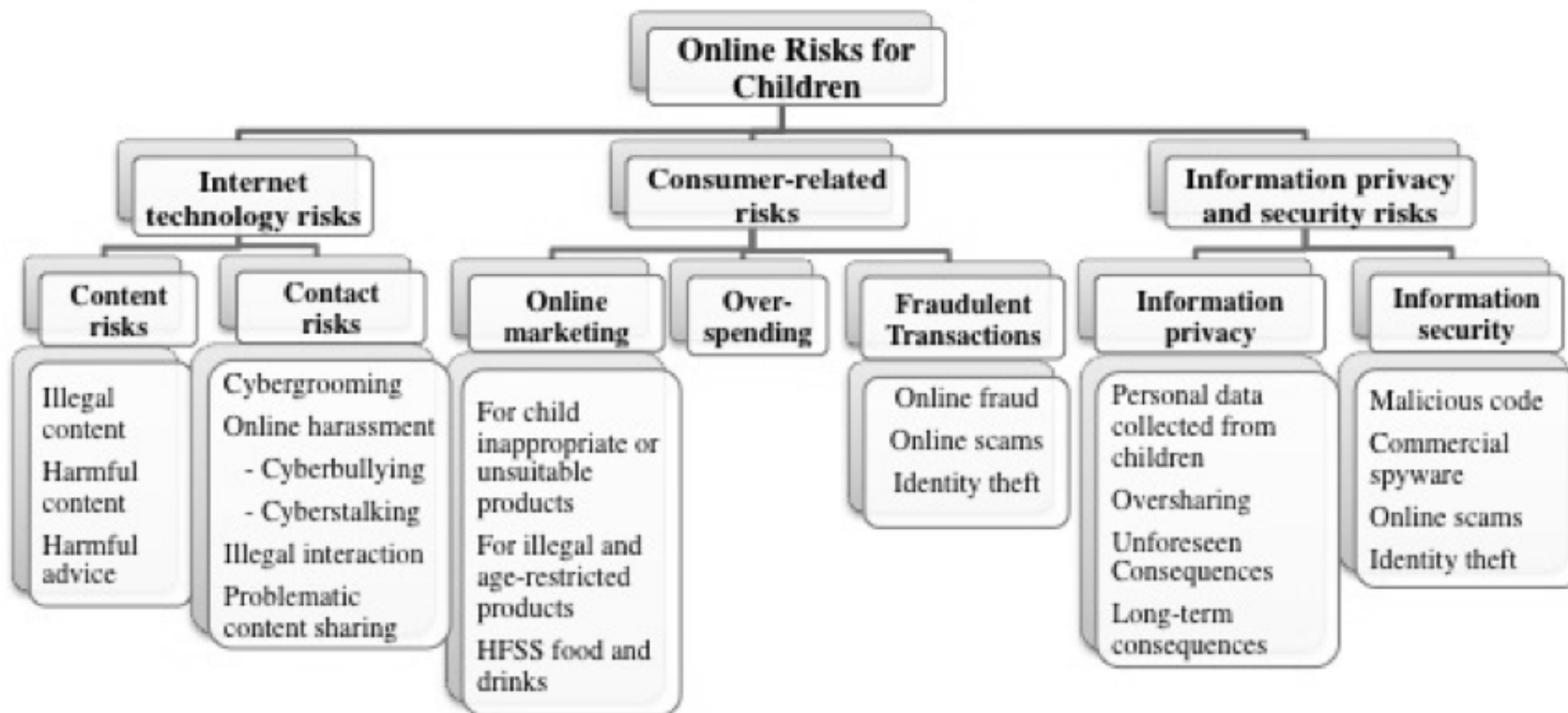
〔資料1〕 インターネットリスキリテラシー指標 (ILAS)

- 総務省は、スマートフォンが急速に普及する中、プライバシーや情報セキュリティ面の課題に対応するため、インターネット上のリスキリテラシーを可視化した「青少年のインターネット・リテラシーに関する指標」(ILAS)を作成。
- ILASのリスク体系は、OECDによるインターネットのリスク体系を元としている。このリスク体系は、汎用性があり青少年に限定されるものではない。
- ILASは、OECDで進められている国際的なインターネットリテラシー指標の整備にも提案されている。従業員のリスキリテラシーが国際的にどの程度のレベルにあるのかを評価することも可能となる。
- 総務省からはILASのリテラシー項目を拡張して使用することが推奨されている。

〔 ILASの公表 (www.soumu.go.jp/menu_news/s-news/01kiban08_02000092.html) 〕

〔資料2〕 OECDのオンラインリスク体系

Figure 7. Typology of risks



(http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en)