システム監査学会　第28回研究大会

〔情報セキュリティ対策の診断研究プロジェクト報告〕

従業員のSNS利用に関する企業の情報セキュリティ対策の研究

―利用場面へのリテラシーチェックリストの適用―

2014年6月6日

情報セキュリティ対策の診断研究プロジェクト
報告者　　木村　裕一

目次

2012年の研究から

- SNS利用における従業員のリスク領域

→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はカバーしない部分が発生

- 発言する従業員のポジションに応じて求められる対応

→（アルバイト、派遣社員）社会人としてモラルある発言

→（経営者）立場を踏まえた発言、クレーム処理の技術

- SNS利用によって顕在化するリスクに変化

→従来、企業がセキュリティの対象としていた情報資産管理

⇒業務プロセスとかけ離れた場所で個人的に情報を発信してしまう

- 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

- チェックリストを用いて診断を実施
- SNSリスクリテラシー向上の施策

→ILAS（資料1，2）のリスク分類を参考にインターネットリスクを見直し

1. 研究の概要 （2013年度の研究）

1．1 はじめに

（1）研究の概要
①SNS利用による炎上など企業が“被害”を受ける例が減少していない。
昨年の研究結果を企業の立場から考えてみる。
② 問題はなぜ発生したのか、その原因がどこにあるのか。
従業員のSNS利用はどのような状況であるか
どのような対策をすれば良いのか。
（2） 研究目的
①企業防衛 従業員のSNS利用により企業が抱えるリスク
・根本の原因は
②企業防衛の立場から、このような問題に対する対策を検討
また予防するための対応を研究

図2　　2013年度の研究結果（概要）

テーマ：企業防衛の立場で従業員のSNS利用の対策を考える

検討過程

①事例から炎上の原因などの追及　　原因　：　従業員の教育不足

②従来の企業の情報システムの対策の範囲になかった

これまでの規定の範囲にSNS利用教育が含まれていない(ことが多い)

アルバイトパート　利用ルールを知らない　教育していない

業務管理ができていない　管理体制なし

③これまでの考え方では対応が不可

企業の対策：予防だけでは限界がある

④炎上(事件・事故が発生する）が避けられない、

発生を前提としてその後の対応を考えておく

⑤企業が被害者とは言い切れない

結論：企業はやるべきこと（コンプライアンス教育、業務管理）をやる必要あり

コンプライアンス教育が重要

成果物　　診断・監査　チェックリスト、診断ハンドブック、セキュリティハンドブック

1．2 SNS利用による事件・事故

炎上などSNS利用による事件・事故は減っていない

(1)事件・事故による企業への影響
（企業の社会的地位の低下、企業イメージの低下など）
企業への信頼の失墜 （客離れ、株価の下落）
企業サービスへの信頼の失墜 （不買、解約・返金要求、契約の解除、客離れ） → 店舗の閉鎖など
企業内情報の漏洩、流出（企業情報管理方法、企業戦略等の見直し）
従業員の処罰、解雇

(2)事件・事故に関わる情報の種類 （企業情報内の漏洩）

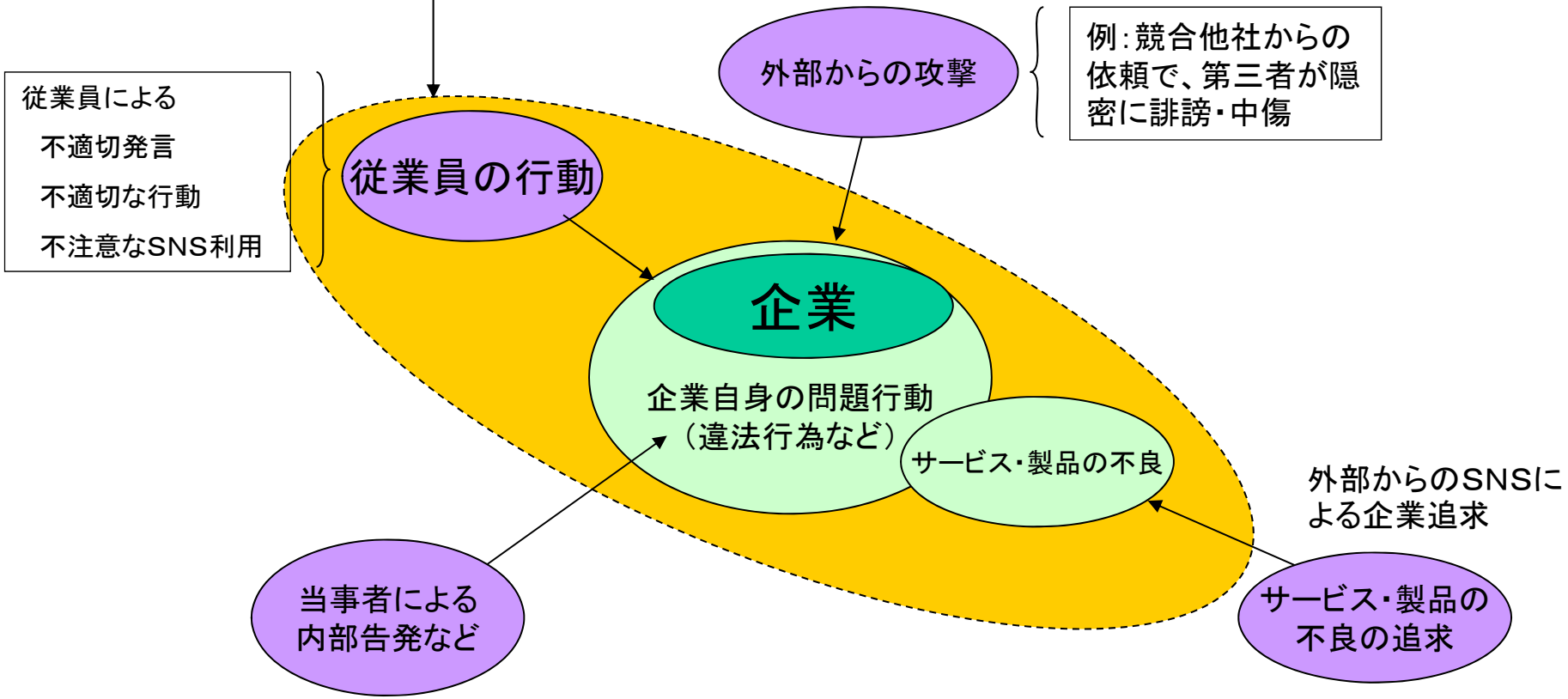
- 顧客情報
- 企業秘密情報（公開すべきでない情報）
  個人情報（本人や他の社員情報）
- 発生させるべきでない行動の情報等
  従業員の不適切な行動情報

事故事例（SNSの特徴的な事例）

事例	ステーキ店の冷凍庫への立ち入り写真の掲載による炎上（2013．8）	回転すし店で、客が醤油用の小瓶を口にくわえた画像を掲載し、炎上
事件の概要	ステーキ店のアルバイト従業員が食材が入っている冷凍庫に腰まで入り、その写真をツイッターに投稿。投稿アカウントはたちまち炎上	店舗備え付けの醤油用の小瓶を口にくわえた画像をTwitterに投稿。
経緯と炎上した結果	ステーキ店のチェーン会社は、食材の廃棄と消毒などを進めたが、顧客の信頼回復は難しいと判断し、その店舗の閉店を決めた。	お詫び文をホームページへ掲載。26日の営業開始前に36店舗で全てのしょうゆケースの中身を廃棄し、洗ってから詰め替えた。同社は「常識を超える行為だ」とコメント
その後の影響	事件が明らかになって休業後、閉店の決定を行うまで1週間。会社は従業員に損害賠償の検討もしている。	醤油の口くわえや鼻への差し込みなど似た事例がその他多数。
類似の例	・コンビニの冷凍庫への立ち入り	餃子チェーン店では、男性客の集団が全裸でカウンター席に座りそれを写真撮影。**同社は該当店舗の閉店**を決定。行為を指示した風俗店社長らが10月に逮捕される

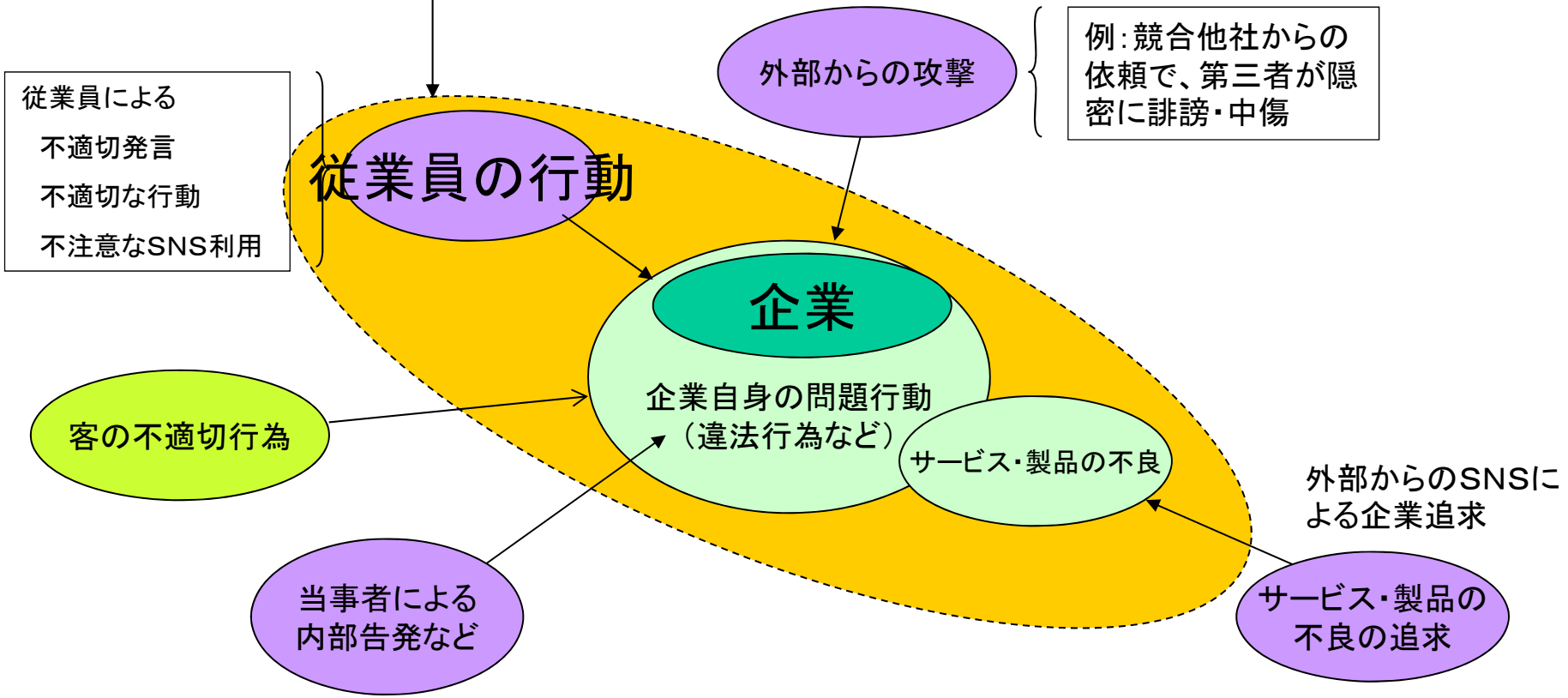
SNS利用に関連して企業が抱えるリスク

- 当研究では**以下の黄色の範囲**を対象にする



SNS利用に関連して企業が抱えるリスク

- 当研究では**以下の黄色の範囲**を対象にする



従業員のSNS利用に関連して企業が抱えるリスクの事例 SNSによる事件・事故分類

事件・事故の要因となる事項	（誰が）何を	どうした	例	被害状況
従業員がSNSにより直接情報を発言・発信	企業内情報 本人情報 他人の情報	社内機密をつぶやく 担当業務と情報を自慢する 来店客の情報を発信	情報として提示 某スポーツ店	本人は退社
	本人の行動情報を掲示	法令、社会規範に違反	無免許運転の告白	
	従業員の不道徳行動情報を本人や仲間が掲示	不衛生な行動情報を広く流布される	ステーキ屋、コンビニの食品冷蔵庫に立ち入り	店舗の糾弾 店舗の閉鎖
友達経由の漏洩	新商品情報	家庭で話した情報を子供がSNSに掲示	某菓子メーカーの新商品企画情報の漏れ	新企画のもれ
成りすましされる	本人情報を漏洩し、なりすましをゆるし情報操作される	企業のひぼう・中傷情報の流布		
匿名（身元を隠し）で	行動情報 他人の写真　を掲載	本人は特定されないと考え、（盗撮写真など掲載）不道徳行為を行う	特定されないと思い、無免許運転を告白	従業員の所属企業が非難される
匿名発言の本人追及	匿名発言の本人が誰か、どこの所属か、身元探し	問題発言の情報の主を探す→特定され本人、家族のプライバシーがあらわになる	過去の発言履歴をサーチ 投稿写真から住所が判明	同上
技術的な不備（ウイルスアプリなど）	安全でないソフトを使用 SNS利用に関わる場所に格納された企業情報	安全対策を行わない 端末内情報の漏洩、企業情報システム侵入の手がかりを与える	PWを盗まれる クレジットカード情報を盗まれる	

１．３ 従業員のSNS利用による企業リスク

（1）事件・事故の原因の分析

SNS利用本人が情報の取り扱いをわきまえず、また誤って発生させた事故・事件

・SNSの基本ルールを知らず利用する

・利用者のコンプライアンスの認識や態度の低下（情報流出は不可であることを承知で匿名で発言する）（投稿、友達にのみ伝えるような認識で発言）

・問題となることをまったく意識しない、羽目をはずした若者の行動

・匿名で発言するので、本人は知られることがないと考える

（2）さらにその原因

SNS利用ルールなどを知らない（影響を認識しない）

SNS利用の留意事項はこれまでの企業規則には直接含まれていない例が多い

（ISMS，Pマーク取得企業においても同様であり、問題発生する）

従来常識にゆだねられていた　それが最近の従業員には確保できず、崩れている

⇒ 従業員のリテラシーの問題と考えられる

1．3 従業員のSNS利用による企業リスク（つづき）

（3）従来の情報取扱い、情報管理と何が違っているか

①SNSでは誰でも、どこからでも情報の取り扱いが可能。その結果、意図的な漏洩等以外に、意図しないで事故を発生させる場合がある

②従来の情報セキュリティ対策への追加項目、情報管理では限界

情報取扱者の限定は難しい

（従来の）企業情報に限定が出来ない

以上の事件・事故の場合、企業は従来の対策を行っているにもかかわらず従業員が事故を発生させ、企業が（本人も含め）被害を受けている

（4）従来の情報セキュリティ対策 （企業情報管理）

①情報システムとして、独立し管理することができた:

・企業情報取り扱い者を限定できる

・情報のアクセスを限定できる、利用状況を管理できる

・取扱い規定をルールとして関係者に周知徹底できる 等

②従来の情報管理方法はそのまま継続している。

従来の情報取扱い、SNS利用の情報取扱いの違い

	問題の発生要因	ルール	情報利用形態		(A)⇒(B)で増加したリスクへの対応
			(A)従来	(B) SNS	
情報	企業情報	情報システム管理規則	情報システムが管理する情報	左に同じ	基本は左に同じ
従業員の行動	従業員(社員)の行動	就業規則	企業の業務管理規則の中で管理が可能	企業の業務管理規則の中で管理が可能。SNSを利用	SNSはプライベートの問題として規制は遅れる、または無
	従業員(パート・アルバイト)の行動	パート・アルバイト社員の就業規則	管理の目の行き届かない場合に問題が発生。しかしその状況が広まることはなかった。	管理の目の行き届かない場合に発生。SNSの利用によりその情報が制限なく世の中に広まる(ことが可能になった)。	企業の立場において問題と考えず、興味に任せて手軽に世間に発言。匿名が可能であるが、問題発言は隠し切れない。またうっかり発言をする。 この部分のリスク対応は新しい分野。対応(ルール整備、業務管理、教育など)はまだ十分でない
	従業員構成の変化とそれに応じた管理 (一般的に)アルバイト・パート社員比率の増加 短期雇用者に対する教育が不足がちになる	パート・アルバイト社員の就業規則 (十分に規定していない。規則を周知できていない。) (SNS利用の留意事項までを就業規則として明確に規定できていない。)	<一般的に> 従業員の目の届く範囲で行動 管理の目の行き届かない場合に問題が発生。しかしその状況が広まることはなかった。	<一般的に> アルバイト・パートに依存する比率が増え、従業員の目が行き届かない場面が増加。不祥事などの問題行動が容易に世の中に発信できる	

２．SNS利用に関する企業のリスク対策
２．１　SNS普及以前と普及後との相違

（１）根本的状況

SNSが普及する以前も以降も、人の行為は変わらない

- 個人が引き起こす問題も、昔から変わっていない
- 個人が考えることを社会に伝える手段が変わっている

（２）SNSを利用することで、利用者の考えることを即時に広範囲にかつ多くの個人宛に記録を伴い伝達が可能。

- これは従来はなかったコミュニケーション手段であり、
  SNSの利用は、コミュニケーションの変革（革命）
- スピード感（所要時間が日単位から即時化）が違う
- あらゆる関係者が参加できるSNSによるコミュニケーションの変化は従来の延長ではない。また、SNSによって発生する事件・事故の対応策は、これまでの管理策では扱えないものになっている

SNS普及以前と普及後との相違

個人の考えることを、相手や社会に伝達する方法

	SNS利用なし（普及以前）				SNS利用
情報伝達の特質	当事者間（主）、社会一般（従）				当事者間、社会一般（差が無くなる）
伝達、手段	手紙	電話	放送	新聞	個人がSNSを行う
スピード（時間の単位）	日	日	準備は：日 伝達は：即時	準備は：日 伝達は：即時	即時、
記録	残る	残らない	残らない	残る	記録（文章、写真、録画）が残る
伝達相手数	1：1	1：1	1：N	1：N	1：N（多数）
伝播 影響力	少	少	大	大	非常に大
発信（誰が）	当事者、関係者（直に）		第三者、記者（途中で人を介す）		当事者、関係者（直に）
受信（誰に）	当事者、関係者		社会（視聴者、読者）		当事者、関係者、社会（SNS、インターネットなど利用者）

２．２ 既存のリスク対策基準と項目

（1）企業防衛を念頭に、以上の事件・事故に関して、対策をISMS管理策、システム監査基準のリスク対応の管理項目ではどのような項目が該当するか。

（対象が情報システムと、従業員の行動全般では適用に無理があるのは承知）

① JISQ27001の管理策における、対応項目

例：7 人的資源セキュリティ ７．１雇用前　雇用者の役割、選考、雇用条件

７．２ 雇用期間中　など

雇用者や従業員管理、教育に関して、具体的な内容を設定しにくい。

②システム監査基準

例：Ⅵ. 共通業務 ４．人的資源管理 ４．3教育 (2),(3),(4)項

＜項目例示＞(2)教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。 等

対策するべきリスクに、どのような対策を検討するか考えにくい

リスク内容をブレークダウンして考えることが、目標に対して妥当（2012年結論の確認）

炎上するケースと炎上に至らないケース

何が違うのか

対応項目	炎上したケース	炎上しかかったが、至らないケース
問題発生の検知	早期に検知できない	早期の検知する
初期消火	速度（対応が遅い） 誠意が見られない対応 （責任者が対応しない） 対応が二転三転する	速度（素早い対応） 誠意ある対応（社長が先頭に立って対処（謝るときは謝る）） 対応が一貫している
応急対策 本格対策　の実行	発見のプロセス――対応ができた のに代表者が対応しない 会社としての課題	企業として状況を把握し、問題の根本対策を行う。 問題の根本対策を短時間でおこなう。プロセスをオープンにする
対応訓練・処理の範囲確認も必要 技術的対処／社会的対処／　心情的対処	実施していない	実施している
例	例：某うどんチェーン店	例：某コーヒー店

２．３　企業防衛のための対策

（１）リスク対策のための項目設定
①企業防衛の立場から考えると、これまで基準としていた
ISMSやシステム監査基準のくくりでは対策を整理し特定しにくい
（注：対象、適用範囲が違うのは承知で比較）
②リスク対策を検討するには、もう少し詳しく項目を分割する必要がある。対策のためには重点指向で考える
③対策を明確にするためには、SNS利用に関してリスクを部分的にブレークダウンしたリスク分析が必要
④（更に）リスクとその対策の整理・体系化を考えることが必要

（２）リスク対策のチェックリスト化
その為のリスクを洗い出し、整理する

（３）（２）リスク対策として新たに考える項目を検討
⇒　チェックリストの作成

3. 企業防衛の立場から成果の利用

3.1 企業の採るべき対策

（1）基本認識の変更 （従来の延長線では対策は出来ない）

本当に企業が被害者？

企業が行うべき対策を実行しなかった結果、と考えるべきではないか

（2） 従業員に対するコンプライアンス意識の教育がこれまで以上に重要

①従業員等に関する教育・訓練

②企業としてのIT環境の変化への対応

②リスクの顕在化は防げない。事件・事故の発生を前提として対策が以前に増して必要

（3）企業防衛のための対策

身近にリスクがあると認めることの認識に立つシステム的（組織的）対策が必要

①発生防止策だけでは対処できない。

事件事故の発生を前提として対処を考える必要あり。

②その対処

・監視・検知

・事件事故対応計画と準備

・炎上の危険性に対応する訓練（SNS固有の対処と一般の不祥事対応がある）

３．２ 成果物

企業が自社のSNS利用状況と問題点を把握するため

（１） セキュリティハンドブック

①チェックリストを基にしたSNS利用に関する留意事項、診断、監査への利用をガイドする

②チェックリストを基にして、必要な対策（ルール）を策定

③チェックリストを基にして ⇒ 企業内教育（内容）（まだ未確定）

（２） 診断、監査

SNSに関するチェックリストを企業診断に適用する

SNS利用による企業のリスクをブレークダウンした。

これを元にしたチェックリストの利用が可能

（３） 評価・診断のためのガイド

リスク チェックリスト ⇒ 企業の対策状況の診断項目に活用する

（診断実施への評価・診断のためのガイド）

４．課題 （今後どれを取り上げるか未定）

（１）従来の延長上で扱えない対策について

３．１項の対策の有効な実施方法は

（２）（企業防衛のための）企業の責任範囲の検討

１）今回はこの企業責任の問題は深く検討していない（未実施）

今回検討の前提：（事件の当事者が所属する）企業の責任を広くとらえる←世間の“あの企業の従業員が”という見方に合わせた

２）本来次をどのように考えるべきか

・従業員自身に帰着／・従業員自身と企業に帰着／企業に帰着

・法律問題と世間の感情的な受取り方の差がある

（３）リスク体系に基づく教育カリキュラム

教育方法と内容

SNS利用のメリット／デメリット（リスク）をセットにした教育

（４）身近にリスクがあると認めることの認識に立つシステム的（組織的）対応策

（現状）（２）から（４）を事業として実施している企業もある

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

情報セキュリティ診断研究プロジェクト
2014年度のテーマ と メンバー募集

テーマ：サイバーディフェンスとシステム監査

- 近年激しさを増しているサイバー攻撃について、その内容をいろいろな視点から研究しシステム監査の役割などを研究課題に取り上げる。

進め方：サブテーマを設定し、その内容の研究を積み重ねてゆくことにする。

〇サイバー事件、事故
〇サイバー攻撃の実態：現状の把握
〇サイバー攻撃の旧型、新型タイプの違い
〇代表的攻撃方法／ 防御方法
〇システム監査の役割

これらのテーマの中では、次のような項目についても、資料などを読み議論する。

〇企業、国の動き、団体などの対応・対策
〇法律、調達基準、国際安全基準の動き

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	• 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	• 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	• 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	• 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	• 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。

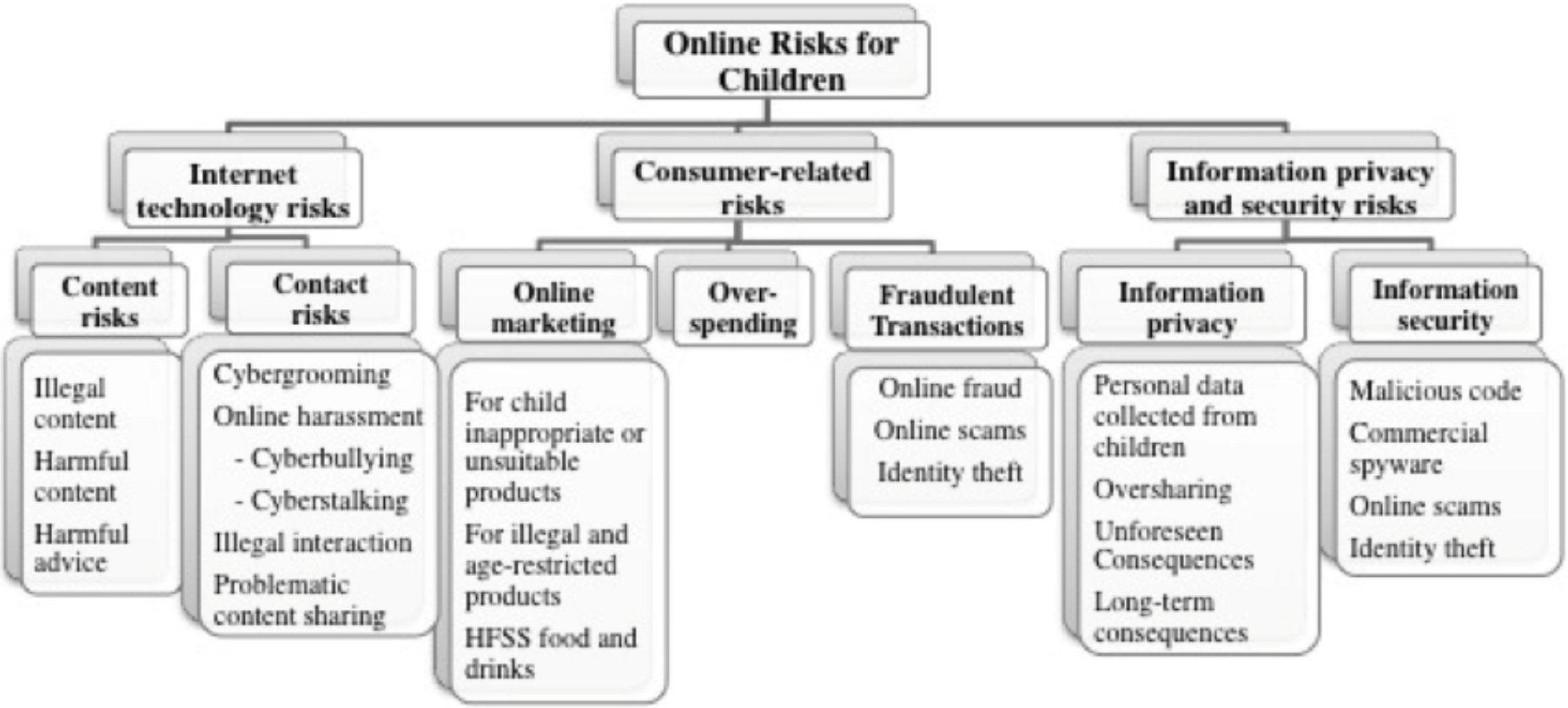
〔資料1〕インターネットリスクリテラシー指標（ILAS）

- 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ク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にしている。
  ILASは青少年のSNS利用時に多発する事件・事故の問題の解決に特化したリスク体系
  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。従業員のリスク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 ）