内閣サイバーセキュリティセンター　発表資料　　平成28年6月1日

中小企業向けサイバーリスク対策の要点

目次

1. 【課題】専門家の指摘する課題（事例） P2

2. 【態勢】内部統制システム と ITプラス･コーポレートガバナンスの定着 P3

3. 【対象】営業秘密の保護、不正競争防止法による対処と国際条約の要請 P4

4. サイバ-リスク総合マネジメントについて の提案 P5

5. サイバ-リスクコンサルタントセンタ-(CRCC)の企画 ・(補足) P6 ～

三井住友海上火災保険株式会社

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

項目　1　専門家の指摘する課題　(事例)

- 中小企業は**踏み台リスク**となることに警戒すべき
- **ターゲット**が中堅・中小企業に**シフト**している
- **政府や民間で**中小企業の対策支援が必要
- サイバ-リスクの**可視化**取組を推進
- **サプライチェ-ン**のパ-トナ-を含めて対策議論が必要

出典　　保険毎日新聞（平成28年3月16日）
東京海上日動社主催　サイバ-リスク研究会

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

項目　2　内部統制システムと ITプラス・コ-ポレ-トガバナンスの定着

詳細は別紙1,2　ご参照

- **中小企業においては、内部統制システム構築が十分でない点が見受られるとの意見が従来からあった。**

↓

- **現代のサイバー社会においては、経営管理の遂行上、IT対応を踏まえた、内部統制＆外部統制（ITプラス・コ-ポレ-トガバナンス）が求められる。**

↓

- **サイバーリスク総合マネジメント(予防・事故対応・補償)の採用は、二つの企業統制システムの向上・定着の手法となる。**

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

項目　3　営業秘密の保護、不正競争防止法の対処 国際条約の要請

詳細は別紙3　ご参照

- サイバ-(攻撃)リスクの対象となる営業秘密は**知的所有権**。

↓

- 不正な盗取は**不正競争防止法**による処罰の対象。

↓

- 保護は**国際条約**による要請。保護実効は日本国の**義務**。

↓

- 攻撃に対して法に基づく処罰対応のためには**証拠**が必要。
  証拠獲得のためには **ログ**や**フォレンジック対応**の確保が必要。
  しかし、中小企業は措置がとれないケ-スも多いと推定される。

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

項目　４　サイバ-リスク総合マネジメントについての提案

詳細は別紙4　ご参照

- **予防対策**と**事故後対策**が、セキュリティ対応の範囲。
  攻撃を受けた後の対応方法・内容・効果も重要検討課題。
  攻撃者**処罰**や**使用差止請求**等の対策実効力確保が必要。
  ＊知財権保全には、タイムスタンプの対応等の別途専門準備が必要です。

↓

- セキュリティとは別に、不測の事故損害に備えて、**補償**も手配。
  金銭的な手当が企業存続のためには必要。

↓

- 予防・事故対策・補償の**三位一体**での連携対策・運営を行う
  サイバーリスク総合マネジメントにより企業経営を守る。

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

項目　5

プレゼン済資料　（平成28年3月31日）　抜粋・一部改定版

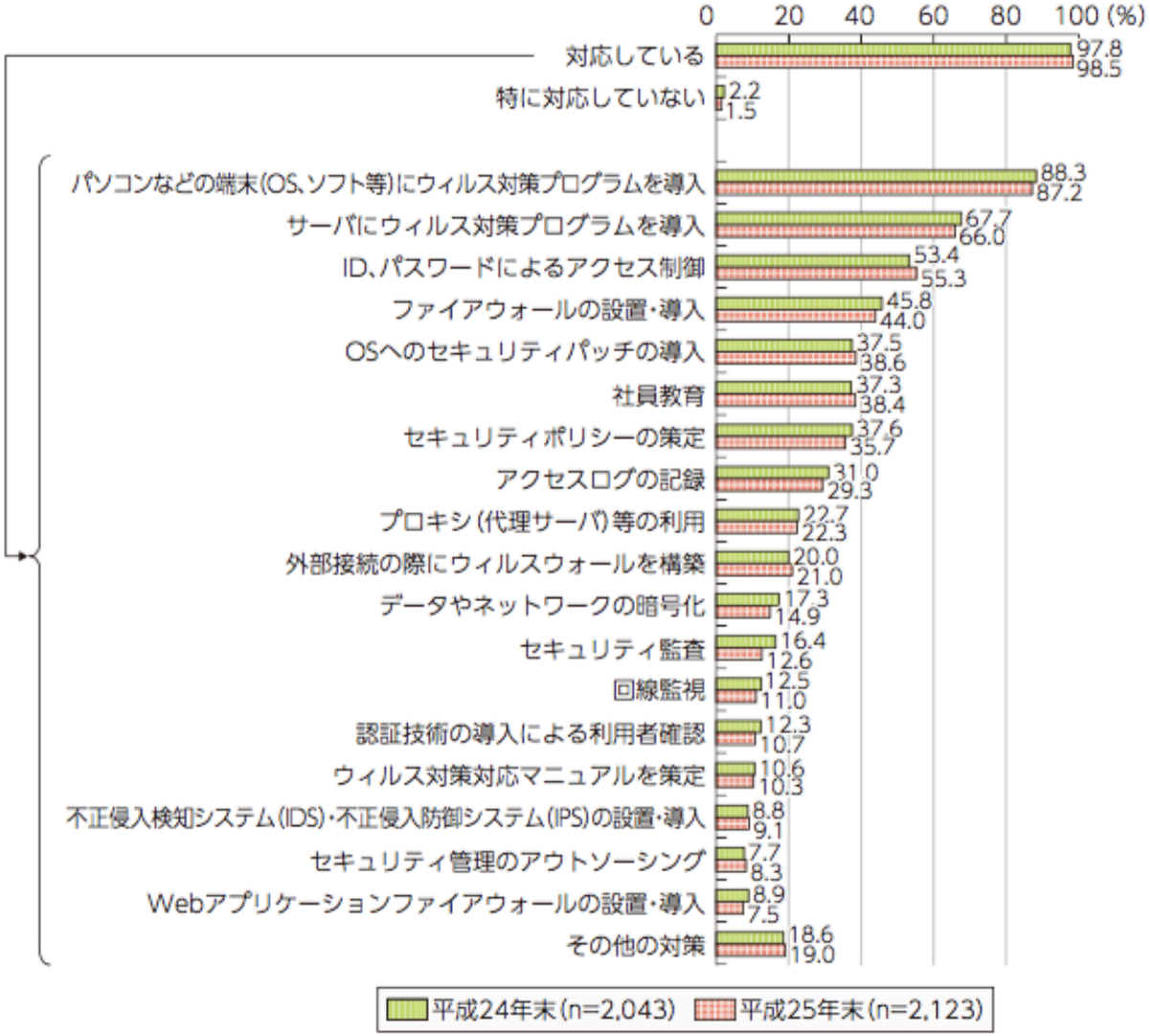
サイバーリスク・事故・損害・保険について

サプライチェーン・サイバーリスクを焦点とした中小企業向けオールジャパンの制度対策(案)

三井住友海上火災保険株式会社

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

企業における情報セキュリティ対策 1



※総務省・H27年版情報通信白書
(http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/pdf/index.html)

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

企業における情報セキュリティ対策 2

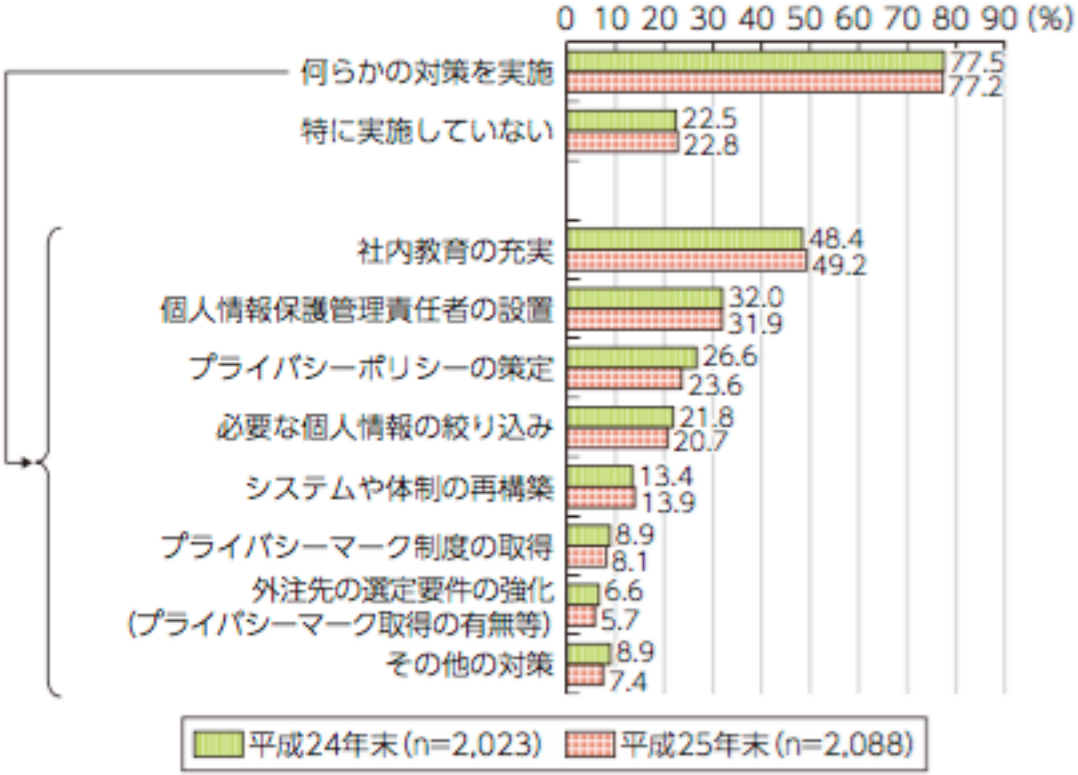
個人情報保護対策

●個人情報保護対策を実施している企業は全体の8割弱

何らかの個人情報保護対策を実施している企業の割合は、77.2%と平成24年末より0.3ポイント減少。

主な対策は「社内教育の充実」が49.2%と最も高く、ついで「個人情報保護管理責任者の設置」が31.9%、「プライバシーポリシーの策定」が23.6%等となっている（左図）

企業における個人情報保護対策の実施状況



（出典）総務省「平成25年通信利用動向調査」
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

※総務省・H27年版情報通信白書
（http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/pdf/index.html）

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバーリスク・事故・保険の現状と課題

【サイバーリスク事故】

1．サイバー事故(加害・被害)は交通事故と類似
　→　注意していても防ぎきれず今後増加、社会的問題として深刻化
2．外部攻撃の抑止が困難
　→　社会全体での防衛体制・意識の継続的強化が必要

【サイバーリスク保険】

切替推進が必要

個人情報漏えい保険　→　情報漏えい保険　→　サイバーリスク保険
（＋法人情報＝営業秘密）（　対象・範囲が拡大　）

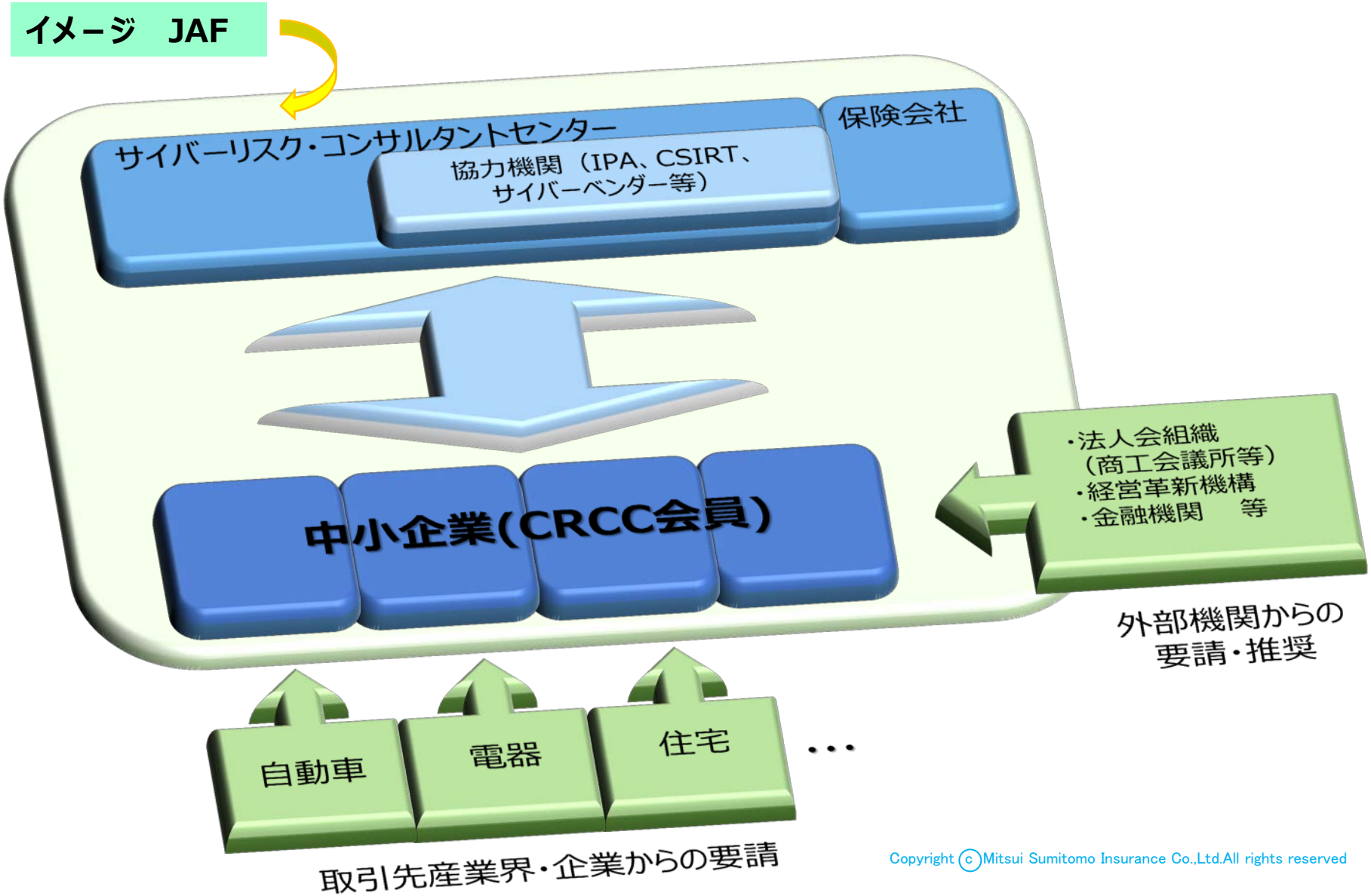
・サイバ-リスクの認識が低い　→　保険の説明・募集が進まない
・サイバ-リスクの対応ができていない　→　保険会社が引き受けられない

実態　サイバ-リスクの予防措置、事故対応、補償が全体として停滞

企業や保険会社の個別対応とは別の視点で検討してみると・・・

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバーリスク・コンサルタントセンター（略称CRCC)(案)

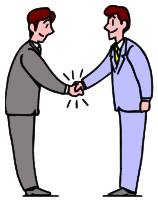


Copyright ©Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

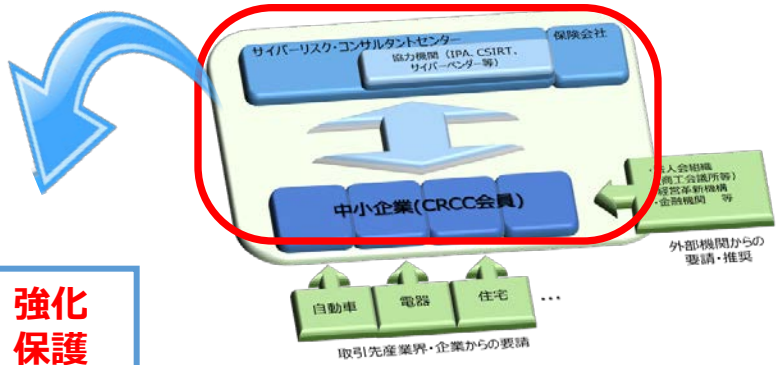
サイバーリスク・コンサルタントセンター (CRCC) ご説明①

CRCCの設置趣旨

官民組織一体化・連携



①中小企業　のサイバー セキュリティ 強化
②大企業　　のサイバー セキュリティ 保護



新制度施策(案)

①【基準】 サイバーセキュリティ認証（サイバー免許証） 制度
②【補償】 全国団体サイバーリスク補償保険
③【態勢】 中小企業向け　ＩＴプラス・コーポレートガバナンス

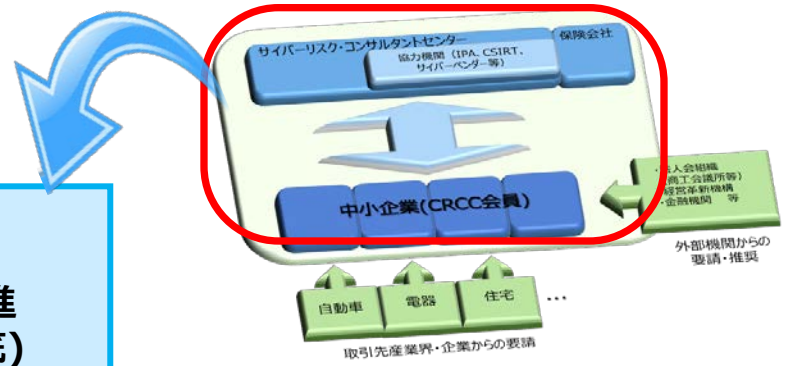
メリット

- **サプライチェーン・サイバーリスク（中小企業→大企業へ波及）の遮断**
- **全国サイバー事故情報の集約一元化と分析・対策の実行**
- **既存組織の融合活動によるサイバー対策コストの低減化追求**

Copyright ⓒMitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバーリスク・コンサルタントセンター (CRCC) ご説明②

業務活動



【管理】

①サイバー事故情報の 収集 → 分析 → 対策 のプロセス対策推進
②重大レベル事故の場合の監査 (詳細な事故情報収集と対策徹底)

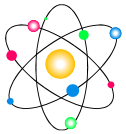
【情宣・相談・指導】

③事故予防と事後対応についての指導 (セミナー・各種媒体での情宣等)
④経営者に対して・・・ＩＴリスクマネジメント・ガバナンス知識の啓発
⑤ＩＴ管理責任者に対して・・・社内のサイバーセキュリティ管理の実践指導

【その他専門施策・対策】

⑥サイバーセキュリティ対策要員の育成・指導の支援活動
⑦サイバーセキュリティ認証制度の実施と運営
⑧サイバーリスク補償保険の実施と運営

多面的に効果浸透

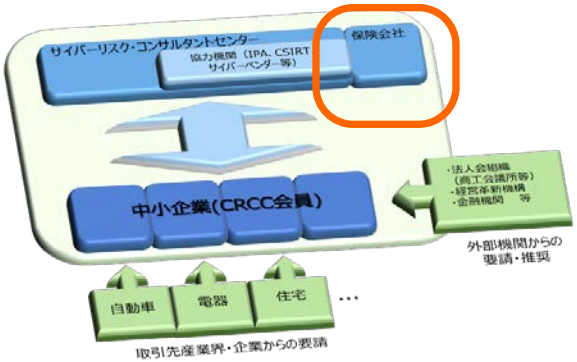


国際取引で日本企業は情報安全性の高い評価

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバーリスク・新保険制度(案)のご説明

【 1． 仕組み (案・概要) 】 ＊特段の新しい内容は含みません



①全国組織法人・中小企業向けの団体保険制度と類似の
　ＣＲＣＣ会員向け制度 (制度やシステムは要事前検討)

②保険料(掛け金)は、年会費として徴収

③加入時のリスク実態チェックは、新認証制度取得で代替

④補償対象リスクは、 (1)個人情報 (2) 営業秘密

⑤保険金種類は、 (1)原因調査、その他の費用保険金
(2)第三者賠償責任保険金

⑥割引率適用想定 ＊割引率は確定事項ではありません

【 2． 構成 】 新保険制度

・小企業
・中堅企業

一定額の必要補償 ＋ 任意で上乗せ補償手配

サプライチェーンリスクが波及しない

・大企業

自社のサイバーリスクのみ保険手配、合理的

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバー攻撃対策としての保険の効用 (シナリオ)

(1)サイバー攻撃　発生。・・・　この段階では、確証無し。???

↓

(2) フォレンジック(原因調査)によるサイバー攻撃の確認。

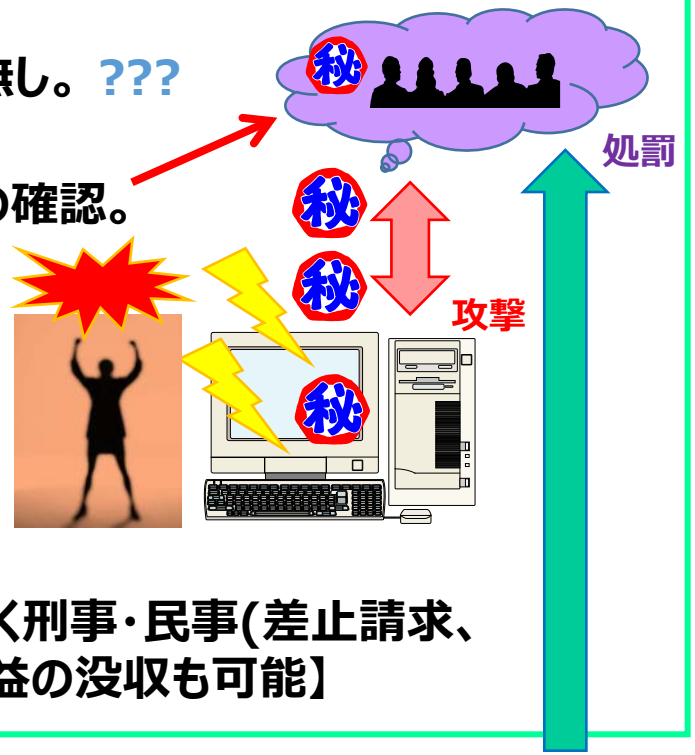
保険金(原因調査費用)を利用

↓

(3) 攻撃情報を記録・分析・対策の策定へ

↓

(4) 営業秘密の不正な盗取に該当の場合　；
攻撃情報を証拠として、不正競争防止法に基づく刑事・民事(差止請求、損害賠償請求)訴訟。【国外犯対応や犯罪収益の没収も可能】



●保険の効果　損害の補償(費用・損害賠償)のみならず、
犯罪の追及と処罰の対策支援として期待。

＊営業秘密の保護は、WTOのTRIPS協定39条の要請です

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバー攻撃リスクの特徴(問題)は

1. 従来の事故・損害経験にはない新しいタイプのリスク
2. 悪意やテロ目的の犯罪行為リスク
3. 個人・法人、誰もが被害対象となるリスク
4. 自社の油断が他社及び他者に迷惑を及ぼすリスク
5. 社会組織の機能や経済活動を広範に麻痺させうるリスク
6. 一次被害者が二次被害者に賠償責任を問われるリスク
7. 攻撃予防措置による安心感が得難いリスク
8. 攻撃情報が集約しにくく、全容がわかりにくいリスク
9. 成功すれば、再犯を招きやすい常習性の高いリスク

このような特徴を持ったサイバー攻撃リスクについては、
組織的かつ継続的な対抗措置と補償の確保が必要です。

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

補足　過去の質問について（ご参考）

Q;サイバ-リスクに関する自賠責制度(含む保険)と同様な制度は設定可能か?

A;難しいと考えています。　＊当社の検討であり、公的な見解ではありません

【理由】

①自賠責制度は特殊な強制加入制度・補償であり、同様な制度の設立は現実的に難しいものと考えられる。

②そもそも自立的なサイバ-リスク対応が企業経営者に求められるところ、強制制度に加入したから安心と思われる可能性も懸念され、リスクマネジメントの趣旨に反するおそれがある。

③被害者の死亡や後遺障害を補償・救済する目的の自賠責制度に対し、サイバ-リスク対応は財産損害に関する企業の賠償責任や費用を補償することが主目的であるから、事情が異なる。

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

サイバ-事故と管理に関する法的背景、想定事項

別紙　1

三井住友海上火災保険
公務開発部　開発室

会社法	348 条 3 項 4 号、施行規則 98 条
一般社団・財団法人に関する法律	90 条 4 項 5 号、施行規則 14 条
金融商品取引法	**上場企業対象、内部統制報告書の内閣総理大臣あて提出の義務**

内部統制システム　；　内部管理体制構築は　**取締役の善管注意義務**である　と趣旨規定されている。

具体的な内容　：　**4 つの目的**達成のために、**6 つの基本的要素**から構成される内部管理体制のこと

【金融庁　**財務報告に係る内部統制の評価及び監査の基準のあり方について**　より】

●**4 つの目的**

1) 業務の有効性と効率性を高めること
2) 財務諸表及び財務諸表に重要な影響を及ぼす可能性のある情報について、信頼性担保に努めること
3) 法令遵守
4) 資産の保全

●**6 つの要素**

1) **統制環境**（内部統制システムの順調な運営）を確保すること
2) **リスク**の分析・評価を行い、適切な対応を行うこと
3) **統制活動**（責任者の明確化と指示実行の手続き確保）を実施すること
4) **情報伝達**を阻害されることなく実行し、正確に組織内に理解させること
5) **モニタリング**（内部統制機能の有効性を確認）を継続して実施すること
6) **IT 対応**（**情報管理規定の策定と適切な実施**）を指揮、実行すること

サイバ-リスク予防・事故管理は、内部統制システムとして取締役に課せられた法上の善管注意義務に該当と解する。

デメリット

1) **コストがかかる　→　コストとの見合いを自主裁量して対応している実態。**
2) 大企業には義務化・指導されているが、**中小企業**に対しては、指針として示されていて、内部統制システム構築は**任意対応**となっている。

・・・中小企業は内部統制システムについて十分な実施がなされていないと推定されている

【リスク対策の実施されていない中小企業で、サイバ-事故が発生した場合のシナリオ】

万一、リスクマネジメントや施策の実施なくサイバ-事故が発生し、自社（含む従業員）・他社（他者）に損害が発生した場合、

1) **当該中小企業の破綻　→　従業員の失業**
2) **役員の善管注意義務違反　→　会社法 847 条に基づく株主代表訴訟等、役員敗訴・賠償確定　→　役員の破産**
3) **他社（他者）の被害者救済の不実行**

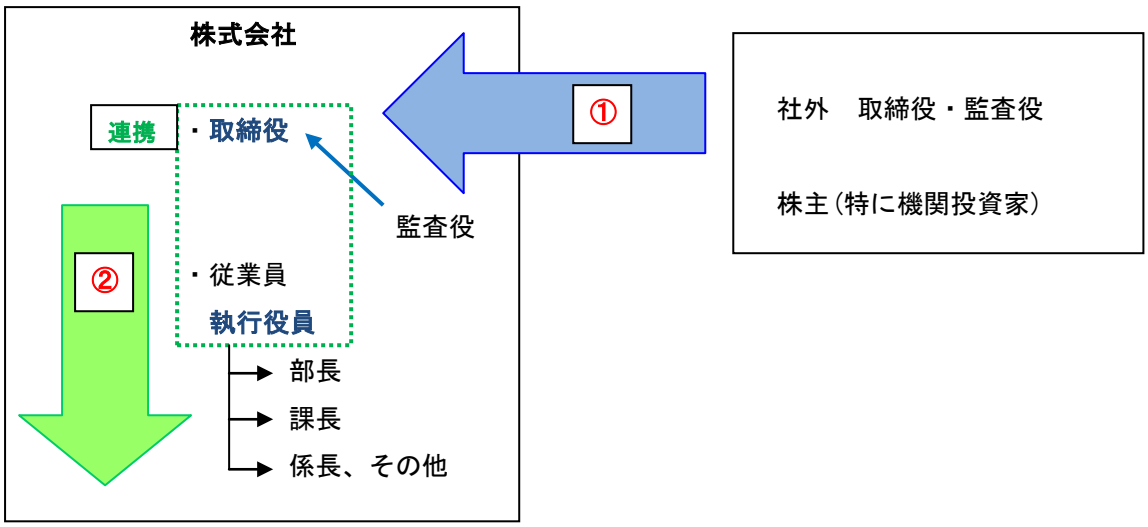
●サイバ-リスクの予防・事故管理と補償の充実のため、新しい法制度を視野に入れた総合安全保障体制の検討

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

会社の仕組み、会社統治システム　（概要）

別紙 2

三井住友海上火災保険
公務開発部　開発室



・取締役　　会社法、商業登記法に定められた役職。意思決定権者。最低１名必要（中小企業は１名が多い）

・監査役　　会社法、商業登記法に定められた役職。社内監査役。取締役の業務執行と会計を監査する。

・執行役員　　法的な要請ではなく、会社の意思決定権者（取締役）と業務執行責任者を分けて運営する場合の役職。取締役会の決定を実行する従業員の代表者・活動の指揮権者との位置づけ。

① **コーポレートガバナンス**

・経営者に対して外部から働く企業統治システム。

・目的は不祥事の防止と収益力の強化。もって、企業の健全な発展と株主等ステークホルダーの保護を図る。

② **内部統制**

・取締役が内部の管理体制を構築し、自らの善管注意義務を果たすことが求められる（**会社法**等）。

・上場企業には、**金融商品取引法**により、内部統制報告書の提出義務が課せられている。
（米国の会計監査制度を法制化した SOX 法にならい、**J-SOX 法**と呼称される）。

・具体的な内容については、金融庁の”**財務報告に係る内部統制の評価及び監査の基準のあり方について**”等において示されている。

●**取締役**は、上記二つの企業統治システムにより、その職責を全うするべく規制される。

●**執行役員**については、取締役に準じ、業務執行責任者として、過失ある場合は損害賠償責任を問われうる。

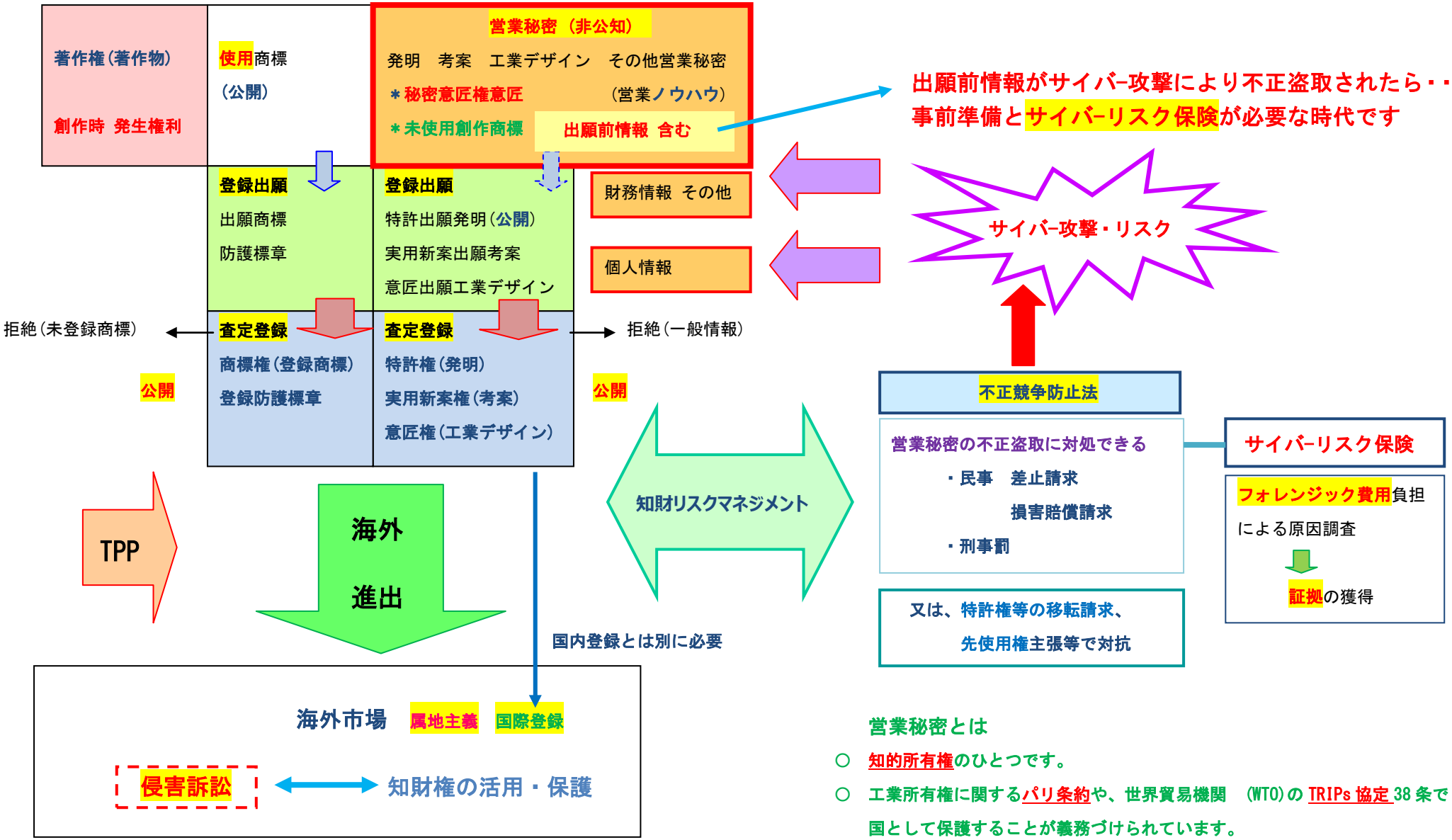
Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

別紙 3

知財リスクマネジメント

三井住友海上火災保険
公務開発部　開発室

知的財産権（特許・実用新案・意匠・商標・著作）・営業秘密　と　サイバー攻撃リスクの関係



営業秘密とは

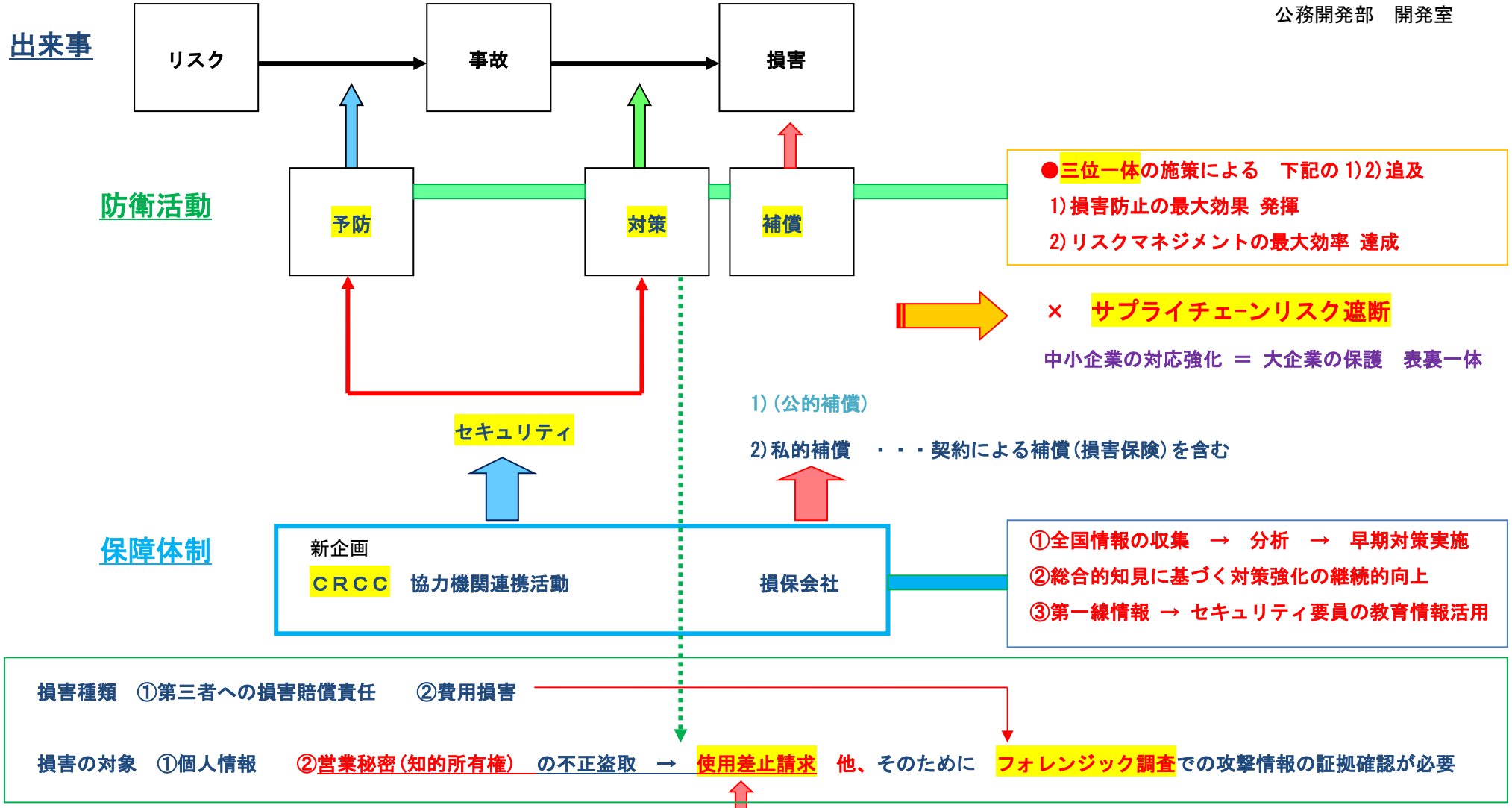
- ○ 知的所有権のひとつです。
- ○ 工業所有権に関するパリ条約や、世界貿易機関　(WTO)の TRIPs 協定 38 条で国として保護することが義務づけられています。

Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

別紙 4

三井住友海上火災保険
公務開発部　開発室

(中小企業)サイバーリスク・マネジメントの図解



・世界貿易機関(WTO)の TRIPs 協定 38 条にて、国内法(不正競争防止法)に基づく営業秘密の保護が義務づけられているので
CRCC による本企画の対応は、日本国が条約を積極的に遵守する姿勢を世界に示すこととなる。

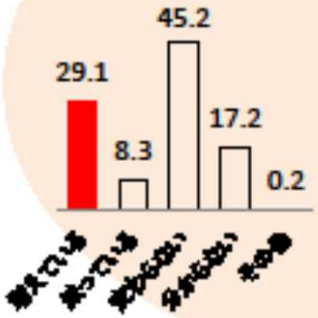
Copyright © Mitsui Sumitomo Insurance Co.,Ltd.All rights reserved

1　改正の背景

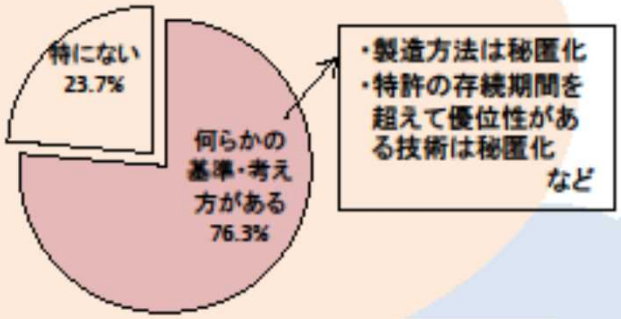
営業秘密の価値の再認識

企業の知財戦略としての「オープン＆クローズ戦略」の広まり
→ 知財の秘匿化（営業秘密）の価値が再認識

＜特許要件を満たす発明をあえて秘匿化？＞



＜知財の権利化・秘匿化に係る考え方＞



（出典）平成26年度経産省「営業秘密保護のあり方に関するアンケート」（540社対象）

営業秘密侵害の危険性の高まり

近年の営業秘密漏えいに関する大型事案の顕在化
- 新日鐵住金vsポスコ（製鉄技術：1000億円の賠償請求）
- 東芝vsSKハイニックス（NAND型フラッシュメモリ技術：330億円で和解）
- ベネッセ（顧客情報：約50社に約3000万件漏えい）

営業秘密侵害事犯（刑事事件）の増加、IT環境等の変化

＜検挙事件数＞

平成25年		平成26年
5件	倍増 →	11件

＜不正アクセス行為認知件数＞

平成25年		平成26年
2,951件	増加 →	3,545件

（出典）警察庁発表「平成26年中における生活経済事犯の検挙状況等について」
国家公安委員会等発表「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」

政府における営業秘密保護強化の検討

平成25年6月　知的財産戦略ビジョン　→「営業秘密に関する制度について検討し適切な措置を講ずる」
→ 知財本部に営業秘密タスクフォースの設置。施策の方向性を議論

平成26年7月　知的財産推進計画2014　→「知的財産戦略本部における最重点5本柱」の1つとして、営業秘密保護強化が位置づけられる

平成26年9月　経済産業省の産業構造審議会知的財産分科会に「営業秘密の保護・活用に関する小委員会」設置
→ 平成27年2月に報告のとりまとめ

出展：「平成27年不正競争防止法の改正概要」（経済産業省）