資料２－４

2018.2.1

三井住友海上火災保険

総務省　情報開示分科会　　第二回プレゼン　　論点の整理

1. サイバー保険

1) 補償概要、付帯サービス等　　別添　資料 1, 別紙ご参照

2) ヒアリングシート　　別添　資料 2 のとおり。　**兼**告知書（違反は保険金不払）。**兼**割引確認資料。

3) 保険の対象 / セキュリティの対象　その違い

保険（補償）	セキュリティ（防止）
・個人情報　不正盗取 ・営業秘密　不正盗取 ※上記は原則。ただし、範囲拡大の可能性あり	・個人情報　不正盗取 ・営業秘密　不正盗取 ・その他企業秘密　不正盗取 ・乗っ取り（含むランサムウェアによる身代金要求） ・サイバー詐欺 ・ソーラーストーム、電磁パルス等の災害による障害

・保険会社の事前の情報聴取活動は、サイバーセキュリティ全体の必要対象情報を網羅しない。

・フォレンジック調査の費用損害は、個人情報と営業秘密の不正盗取（不正アクセス）の合理的なおそれについて補償されるが、乗っ取りや詐欺については、機器の調査が必要としても保険の補償対象ではない。

注）乗っ取り・脅迫等の攻撃は不正アクセスの**おそれ→調査必要**ではなく、明確に犯罪被害が認識される。

2. サイバーセキュリティ情報開示

重要な論点

1) 趣旨

・**現状**　取引先の与信判断は財務諸表等による。与信判断により、取引の可否や取引金額等が決まる。

今後　取引先のサイバーセキュリティ判断は、よりどころがない。

しかし、サイバーセキュリティの脆弱な企業は、本来、取引先適格を喪失しているはずである。

通商・取引の安全性担保のためには、取引先サイバーセキュリティ情報の事前確認が必要。

↓

・世の中に対して、サイバーセキュリティ情報を自ら開示（以下、**セキュリティ与信公開**）を行う要請がある。

2) 効果

・非上場企業を含む企業がセキュリティ与信公開を行うことで、比較されて、より高いセキュリティの企業は取引先として優位になり、競争力が高まる。

よって、セキュリティを高める**自助努力**が自然と形成され、セキュリティが**投資として経営上、認識**される。

3) 目的

・上記の効果によって、**サプライチェーン上のサイバーリスク耐久力が全体として向上**することが期待される。

その他論点

4)検証

・一方で、セキュリティ公開の事実・内容に**不備・偽証等**がないか、チェックが必要。
　→　経営監査の一項目として位置付けることも一案
・専門機関の**外部評価(スコアリング)**による別手法でのセキュリティ与信の確認も**併行して活用**すべき。
いわゆる**多面的与信評価**の実施。

5)運営

・セキュリティ与信公開は、**継続的**に実施され、かつ、不継続については**リマインド**がなされるべき。

6)基準(仮称　**セキュリティ与信開示ガイドライン**)

・公開情報として比較される以上、一定の基準が定められ、**数値や特性等の要素からセキュリティ品質の比較がしやすい**状況が望ましい。
・基準自体も**継続的に更新**され、陳腐なものとならないように必要な協議がなされなければならない。

ご提案

7)普及推進・実効性の確保

・中小企業を主体とする会員制組織 **サイバーリスク・コンサルタントセンター　(略称 CRCC)**において、
会員規約として、**セキュリティ与信開示ガイドライン**の対応徹底を推進する。
すなわち、**セキュリティ与信開示ガイドライン**の情宣、内容の説明、セキュリティ確保の援助、公開の支援、未更新の場合のリマインド　等を、CRCC が会員向け活動として実施する。

● 参考資料　　別紙　3～5　　**CRCC についての説明**