資料５

NISC

National center of Incident readiness and Strategy for Cybersecurity

セキュリティマインドを持った企業経営に係る検討

2016年４月28日

内閣サイバーセキュリティセンター（NISC）
http://www.nisc.go.jp/

IoT時代のビジネスとサイバーセキュリティの関係を如何に考えるべきか

「サイバーセキュリティ戦略」（平成27年９月４日閣議決定）より

５．１　経済社会の活力の向上及び持続的発展

企業が、IoTシステムを通じて新たなサービスを提供するに当たっては、市場における個人・企業が当該サービスに期待する品質の要素としての安全やセキュリティ、すなわち「セキュリティ品質」が保証されていることが前提である。このため、IoTシステムの提供するサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減していくことが、今後の社会全体としての課題（チャレンジ）となる。

「サイバーセキュリティ人材育成総合強化方針」（平成28年３月31日サイバーセキュリティ戦略本部決定） より

第1章　社会で活躍できる人材の育成

１．人材の需要と供給の好循環の形成

経営層においては、サイバーセキュリティに係る取組が経営戦略における不可欠な事業であることを認識し、その推進のために必要な人材を確保し、これらの人材が活躍できるキャリアパスを実現していくことが求められる

経営層の意識改革①(「費用」から「投資」)

「サイバーセキュリティ戦略」より

5．1．2　セキュリティマインドを持った企業経営の推進
(1)経営層の意識改革
　こうした社会の変化をより多くの企業経営層が的確に認識し、セキュリティ対策はやむを得ない「費用」ではなく、より積極的な経営への「投資」であるとの認識を醸成していくことは、我が国の経済社会の活力の向上及び持続的発展のために必要である。

「サイバーセキュリティ人材育成総合強化方針」より

第1章　社会で活躍できる人材の育成
2．経済社会の変化に対応した経営戦略
(1)「経営層」の意識改革(人材の需要の喚起)
　今後、安全なIoTシステムを活用した新規事業や既存ビジネスの高度化に伴い、サイバーセキュリティの確保が利用者から求められることから、企業等がサイバーセキュリティ対策に取り組んでいることをステークホルダー等に情報発信する方策等について検討

「企業価値を高めるサイバーセキュリティ投資」の“考え方”の構築
－“情報化”により生み出される価値とその防護
－ 企業価値、市場価値を高める取組
　(「セキュリティ品質」とブランド価値)
－ 企業における取組についての積極的な発信　等

IoT社会が進展する中で、セキュリティ品質の実現が企業価値になるのではないか

IoT社会の進展

PC

多くの職場・家庭に普及し、インターネットに接続
（2014年末：PC普及率 78.0%、インターネット普及率 82.8%）
※2015年版情報通信白書（総務省）

スマートフォン

世帯保有率が4年間６倍に急増
（2010年末：9.7%→2014年末：64.2%）
※2015年版情報通信白書（総務省）

自動車

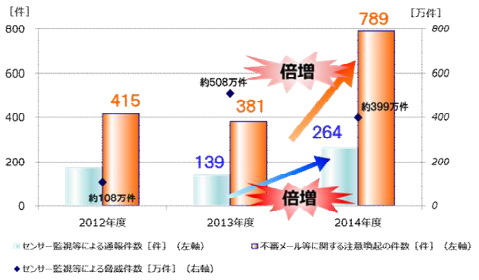
一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行
※自動車の情報セキュリティへの取組みガイド（2013.8 IPA）

スマートメーター（次世代電力量計）

電力会社による開発・導入の開始
［主な予定］
・東京：2020年度までに2700万台の導入完了
・関西：2022年度までに1300万台の導入完了

サイバー攻撃の現状

【政府機関への脅威件数等】



※ GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により、各府省庁等に置かれたセンサーが検知等したイベントを通知した件数。

出展：
NISC「サイバーセキュリティ政策に係る年次報告（2014年度）」（2015年7月）

【IoTシステムへのサイバー攻撃事例】

- 2015年7月、セキュリティの研究者がクライスラー社の「コネクテッドカー」システム（スマホを使ってエンジン起動やGPSで車の現在位置を把握することができるシステム）の脆弱性を突いてハッキングできることを証明。
- 具体的には、第三者がスマホを使って遠隔操作でエンジンを切ったり、ブレーキ操作が可能。
- 同社は、約140万台をリコール。

出典：Wired Magazine

【インフラ・産業基盤への攻撃の海外事例】

○製鉄所の溶鉱炉損傷(ドイツ、2014年)
標的型攻撃により、製鉄所の制御システムを不正操作。
溶鉱炉が損傷。

○ウクライナの大規模停電(2015年)
標的型攻撃により、制御系システムを不正操作。
ウクライナ西部数万世帯で、3~6時間にわたる大規模停電が発生。

出典：
産業構造審議会　新産業構造部会（第7回）資料

・様々なモノがネットワークに接続（IoT）
・サイバー空間と実空間が融合
・IoTシステムを通じて新たなサービスを提供
⇒**セキュリティ品質（安全、セキュリティ）の保証が前提**

セキュリティ品質の実現が企業価値に

サービスの効用（ベネフィット）
比較
セキュリティリスク
・法令遵守
・社会的受容
「費用」から「投資」へ
より高いレベルのセキュリティ品質の実現
・企業価値
・国際競争力

・サービスの効用と比較してセキュリティリスクを許容し得る程度まで低減
・高いレベルのセキュリティ品質の実現が**企業価値や国際競争力の源泉に**

経営層の意識改革②(リスクマネジメント)

「サイバーセキュリティ戦略」より

5．2　国民が安全で安心して暮らせる社会の実現

機能やサービスを全うするという観点からリスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証(任務保証)」の考え方に基づく取組が必要である。

「サイバーセキュリティ人材育成総合強化方針」より

第1章　社会で活躍できる人材の育成

2．経済社会の変化に対応した経営戦略

(1)「経営層」の意識改革(人材の需要の喚起)

社会の変化をより多くの企業経営層が的確に捉え、危機意識を持ってリスクマネジメントに当たることが必要である。

(2)「橋渡し人材層」の育成

経営層と実務者層との間のコミュニケーションの支援を行う橋渡し人材層が経営層に対し、サイバーセキュリティに係るビジョンの提示等の際にコミュニケーションを取りやすくするためのツールとして、具体的な事例を交えたコンテンツを作成する。

“考え方”の実装のためのツール

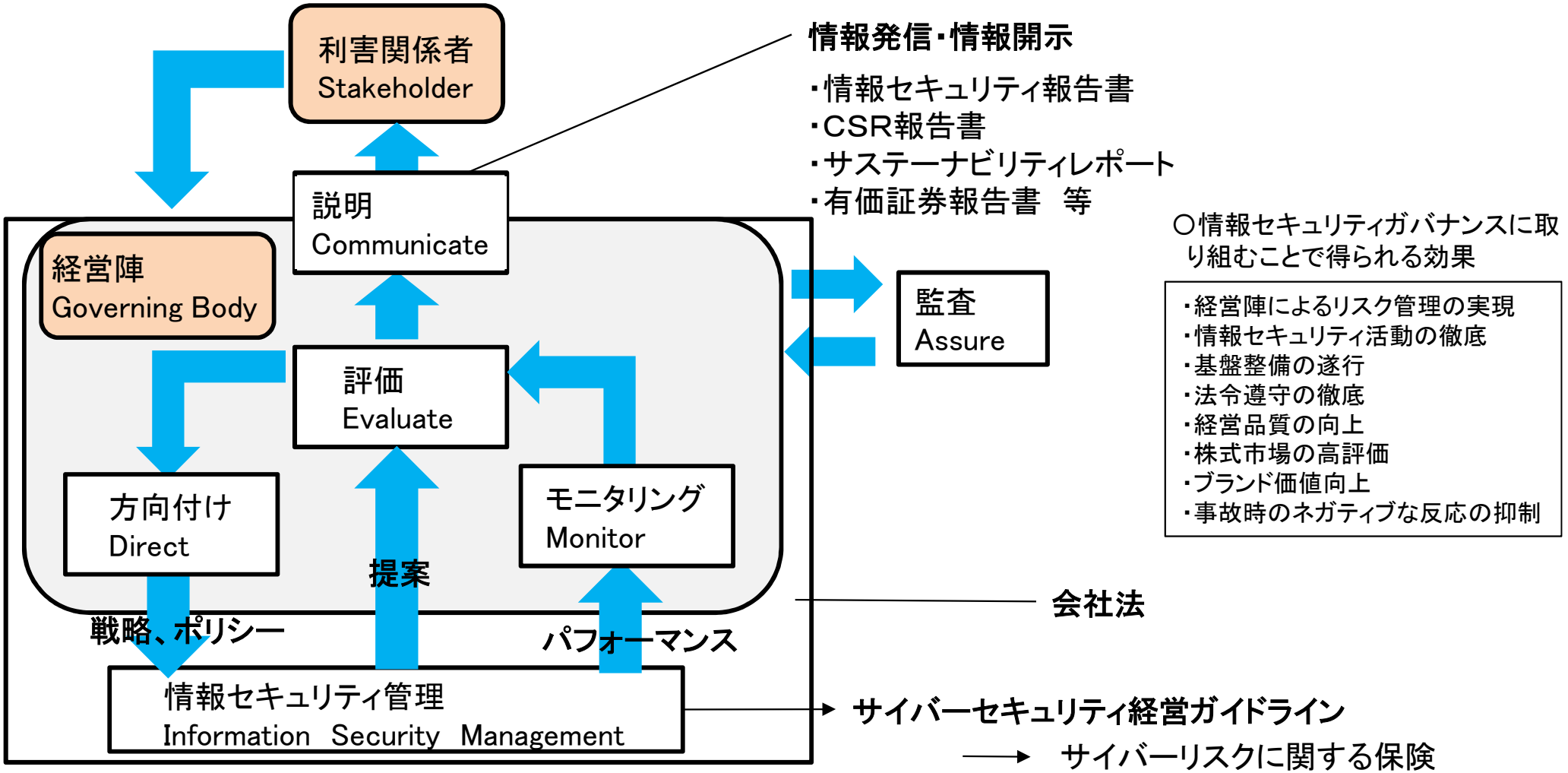
ー経営層の認識を高めるコンテンツ作成
ーケースメソッドの開発
ー情報発信・開示手法の整備
ー取締役会の権限・責務(会社法)

○リスク対策
ー経営ガイドライン(経済産業省)の普及・促進
ーセキュリティガバナンス
ーサイバーリスクに関する保険　等

情報セキュリティガバナンス※の確立に取り組むことで様々な効果を得ることができるのでないか

任務保証の考え方について

業務責任者（任務責任者）がシステム責任者（資産責任者）と、機能やサービスを全うするという観点からリスクを分析し、協議し、残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証（任務保証）」の考え方に基づく取組が必要。



○情報セキュリティガバナンスに取り組むことで得られる効果

・経営陣によるリスク管理の実現
・情報セキュリティ活動の徹底
・基盤整備の遂行
・法令遵守の徹底
・経営品質の向上
・株式市場の高評価
・ブランド価値向上
・事故時のネガティブな反応の抑制

（出典）ISO/IEC27014：2013　及び情報セキュリティガバナンス協議会ホームページを参考に作成

※情報セキュリティガバナンス：経営者が組織内の状況をモニタリングし方針を決定する仕組み及び利害関係者に対する開示と評価の仕組み

情報開示状況（日経225社）

平成25年度 日経225社-業種別サイバーセキュリティ情報開示状況

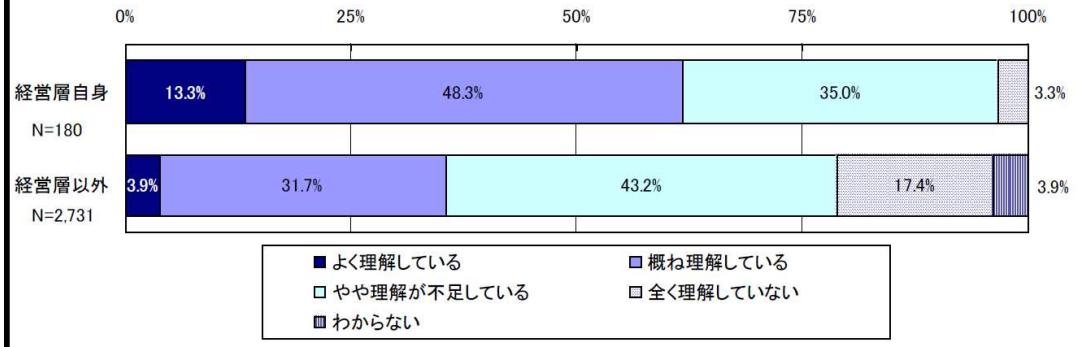
日経業種分類				開示企業数	開示企業%	
大分野	（社数）	中分野	（社数）		中分類	大分類
A 技術	57	01 医薬品	8	2	25.0%	61.4%
		02 電気機器	29	20	69.0%	
		03 自動車	9	4	44.4%	
		04 精密機器	5	3	60.0%	
		05 通信	6	6	100.0%	
B 金融	21	06 銀行	11	11	100.0%	100.0%
		07 その他金融	1	1	100.0%	
		08 証券	3	3	100.0%	
		09 保険	6	6	100.0%	
C 消費	28	10 水産	2	1	50.0%	85.7%
		11 食品	11	10	90.9%	
		12 小売業	8	8	100.0%	
		13 サービス	7	5	71.4%	
D 素材	64	14 鉱業	1	0	0.0%	32.8%
		15 繊維	5	0	0.0%	
		16 パルプ・紙	3	0	0.0%	
		17 化学	18	5	27.8%	
		18 石油	2	2	100.0%	
		19 ゴム	2	1	50.0%	
		20 窯業	9	3	33.3%	
		21 鉄鋼	5	0	0.0%	
		22 非鉄・金属	12	5	41.7%	
		23 商社	7	5	71.4%	
E 資本財・その他	35	24 建設	8	4	50.0%	51.4%
		25 機械	16	8	50.0%	
		26 造船	2	2	100.0%	
		27 その他製造	3	3	100.0%	
		28 不動産	6	1	16.7%	
F 運輸・公共	20	29 鉄道・バス	8	7	87.5%	85.0%
		30 陸運	2	2	100.0%	
		31 海運	3	1	33.3%	
		32 空運	1	1	100.0%	
		33 倉庫	1	1	100.0%	
		34 電力	3	3	100.0%	
		35 ガス	2	2	100.0%	
合計	225		225	136		

出典：
民間企業のサイバーセキュリティリスク開示に係る動向等について
（平成26年度内閣官房委託調査）

サイバーセキュリティ事案を自社で同様の事案が発生した場合の影響として考えてもらうことが有効ではないか

経営層の情報セキュリティに係る認識には経営層自身と経営層以外でギャップがある

Q.自社向けセキュリティに対する経営層の認識・理解について、どのように感じますか。



出典:独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2012年4月

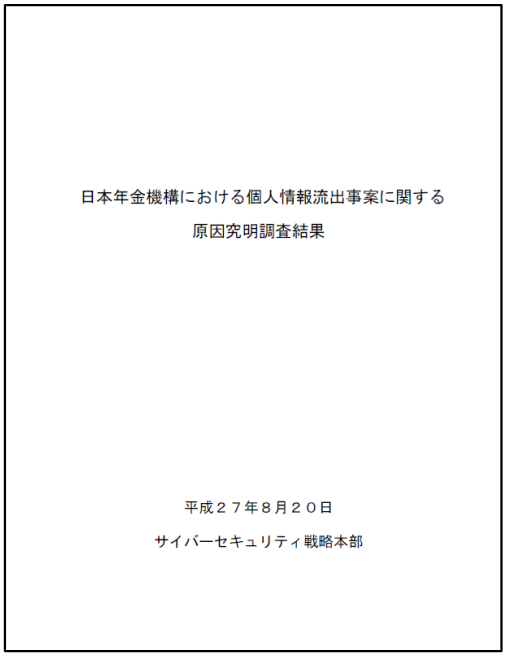
企業等における情報漏えいインシデントの深刻化

	2014年データ	2013年データ
漏えい人数	4999万9892人	925万4513人
漏えい件数	1591件	1388件
想定損害賠償総額	1兆6642億3910万円	1438億7184万円
一件当たりの漏えい人数	3万2616人	7027人
一件当たり平均想定損害賠償額	10億8561万円	1億924万円
一人当たり平均想定損害賠償額	5万2625円	2万7707円

出典:2014年度 情報セキュリティインシデントに関する調査報告～情報漏えい編～（日本ネットワークセキュリティ協会(JNSA)）
2014年1月1日～12月31日の1年間にインターネットニュース等で報道されたインシデントの記事、組織から公表されたインシデントのプレスリリース等をもとに集計。想定損害賠償額については、JNSAが開発したモデルを用いて推定。

・経営層の認識を高めるコンテンツ作成
・ケースメソッドの開発　　等

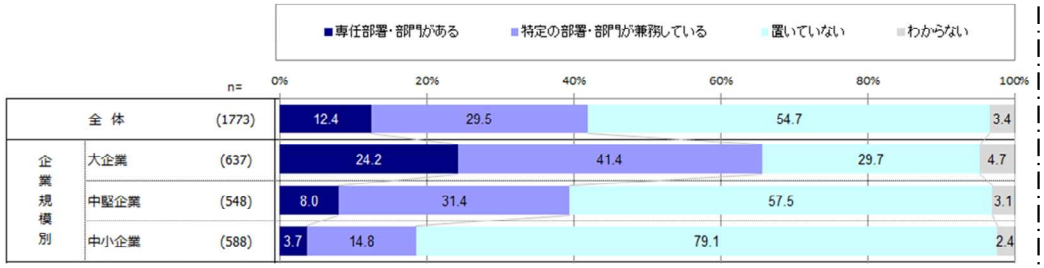
年金機構事案（27年5月）の例


日本年金機構における個人情報流出事案に関する
原因究明調査結果

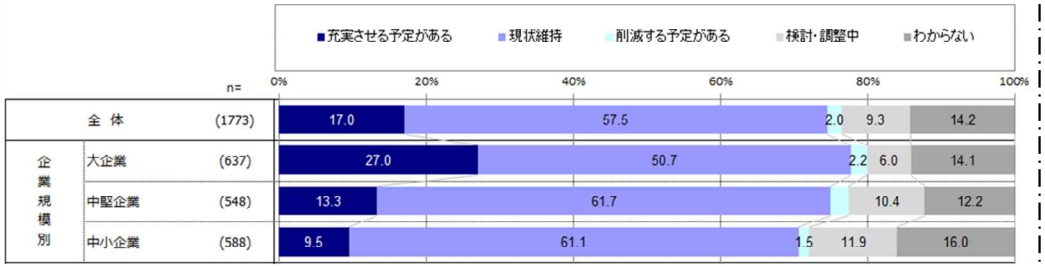
平成２７年８月２０日
サイバーセキュリティ戦略本部

サイバーセキュリティへの認識や取組の違いを踏まえて考えることが必要ではないか

Q. 貴社では、情報セキュリティ管理の担当部署・部門を置いていますか。（1つ選択）



Q. 情報セキュリティ対策について、今後、予算や体制等を充実させる予定がありますか。（1つ選択）



出典：企業におけるサイバーリスク管理の実態調査2015（IPA）

大企業と中堅企業、中小企業とを比較すると、情報セキュリティ管理の担当部署・部門の設置状況や情報セキュリティ対策を今後充実する予定のある割合が、大企業は高い。

企業タイプ別の取組が必要でないか

○今後の取組方針

①IoTを積極的な（グローバル）事業戦略上に位置づけセキュリティを積極的に競争力に位置づけている企業

・データの積極的な活用も含めて、その製品・サービスの「セキュリティ品質」を一層高めるべく、プラットフォームのセキュリティ向上、データの保護、製品等の安全・品質向上に取り組むことの必要性を唱える。その際には、特に、機能保証の考え方を経営層へのインプットとなるコンテンツを作成するとともに、セキュリティを安全基準等に組み込んだ基準・標準等の整備をしていくことをアウトプットとしてはどうか。取組状況の情報発信（手法）も有効なツールと考えられる。

②IT化・セキュリティについて基盤として捉えている会社（概念的に、IT化・セキュリティの必要性は理解しているものの、積極的な活用までは位置づけられていない）

・コンプライアンス（会社法なども含む）や脅威・リスク判断の事例集などを作り、経営層に認識を高めるとともに、経済産業省の経営ガイドラインを普及していってはどうか。また、サイバーリスクに関する保険などもそのツールの一環として考えられる。

③なんとなくIT化している会社（従来型の中小企業や中堅企業等）で、属人的なIT化、セキュリティ対策を実施している会社

・自らセキュリティ対策などを推進するのは困難なところであり、セキュリティが確保されたクラウドの活用等を推進する。なお、クラウドが千差万別なため、適切なクラウドの選定に資する環境整備などが必要になるのでないか。また、サイバーリスクに関する保険などもそのツールの一環として考えられる。