サイバーリスクも経営者の責任

2016年4月2日
林　紘一郎
情報セキュリティ大学院大学教授
サイバーセキュリティ戦略本部員
会社役員育成機構{BDTI}理事

米中首脳会談

近田
「アメリカのオバマ大統領と中国の習近平国家主席が会談し、焦点のサイバーセキュリティーについて、サイバー攻撃で企業の情報を盗む行為をしないことで合意しました。」

（出典）http://www.nhk.or.jp/ohayou/marugoto/2015/09/0926.html

米メディアは米中首脳会談で合意したサイバー問題に関する対話メカニズム構築などの措置に抑止効果があるかを疑問視している。保守系、リベラル系のメディアで会談の評価に温度差はあるが、南シナ海で進められる人工島建設も含めた中国の行動を野放しにすれば米国の国益に禍根を残すことになるという見方では一致している。

http://www.sankei.com/premium/news/151003/prm1510030019-n1.html

METIとIPAの報告書

- 『サイバーセキュリティ経営ガイドライン』
- 2015年12月28日、version 1.0
- METIとIPA合同の研究会「サイバーセキュリティリスクと企業経営に関する研究会」の成果

羅針盤

林 紘一郎(はやし こういちろう)
情報セキュリティ大学院大学教授

サイバーリスクも経営者の責任

暮れも押し迫った12月28日に、経済産業省と情報処理推進機構に設置された研究会（筆者も委員の1人）が、「サイバーセキュリティ経営ガイドライン」を発表した（経産省HP参照）ので、主旨を紹介しご参考に供したい。

今日ではサイバー事件や事故が、メディアを賑わさない日はない。原因は過失によるものもあるが、悪意を持った攻撃も増えている。身近な個人データの漏えいなどは注目され易いが、知的財産の窃取や制御系システムの機能低下まで、あらゆる企業活動が攻撃対象になっている。これらを防止できない主たる理由は、攻撃側と防御側の「非対称」にある。攻撃側は「一点突破」を狙い、大した費用もかけずに個人データや知的財産が手に入れば、こんな「効率的」なビジネスはない。経済的利益を狙わないで政治信条などを訴える場としても、サイバー攻撃は格好の手段である（いわゆるイスラム国の例）。攻撃手段は合法・非合法を問わず簡単に入手でき、攻撃の痕跡を残さない方法もある。対する防御側は、あくまでも合法的な手段で「全面防御」を迫られるにもかかわらず、相手を特定するのに困難があるため、不利な状態におかれている。加えて企業活動の大部分が、情報通信技術（ICT）に依存しているため、サイバーを捨ててリアルな世界に戻ることはできない。

その結果、サイバーセキュリティ対策は、主として利用者の負担で行われている。個人ユーザも、SPAMメールの除去や、アンチ・ウィルス・ソフトの更新を「自己責任」で行わねばならない。企業においてはさらに、システムを切り分ける壁（ファイア・ウォール）を設けるなどの対策を、自社だけでなくサプライ・チェーンに関連する企業間でも維持し、業務委託先にも目を配ることが求められる。しかしITに長けた社員を擁する大企業でも、ITが本業でなければ自前で実施するには限界があり、ましてや中堅・中小企業はセキュリティ専業者に任せるしかない。既に欧米ではMSSP（Managed Security Service Provider）が注目され、わが国も早晩その方向に進むだろうが、それでも安心はできない。システム開発でも良くあるように、「丸投げ」してしまうと時間が経つうちに細部が分からなくなり、ノウハウを含め業務の流れ全体を相手に依存する結果になる懸念もある。外部委託はしても、肝心の要求仕様は手元に握っておかねばならない。

このような時代になれば、企業経営者は従来とは違った視点から、業務をチェックする必要が生じてくる。この分野には、国際標準としてセキュリティ実務家向けの手順書はあったが、今回の「ガイドライン」は経営者向けの初めてのチェック・リストと言える。冒頭には、経営者が認識する必要がある「3原則」と、セキュリティに責任を持つ担当幹部（CISOなど）に指示すべき「重要10項目」が要領よくまとめられている。「そんな暇はないよ」という「食わず嫌い」だけはご遠慮いただきたい。なにせ、昨年9月に行われた米中首脳会談においてさえ、南沙諸島問題とサイバーセキュリティが2大トピックになり、「企業情報を盗むような行為はしないし助けない」という合意を見たほどである。サイバーに関する問題は、今やトップの責任事項になったのである。

経営者が認識すべき「3原則」

- 経営者がリーダーシップをとって対策を推進すべき
- 自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要
- 平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要

責任者となる担当幹部（CISO等）に指示すべき「重要10項目」（1）

指示１：方針（セキュリティポリシー）を策定

指示２：適切な管理体制の構築と、責任の明確化

指示３：セキュリティリスクの洗い出しと、対処計画の策定

指示４：PDCAの実施と、経営者への報告、ステークホルダーへの適切な開示

指示５：系列企業やサプライチェーンのビジネスパートナーを含めた実施

責任者となる担当幹部（CISO等）に指示すべき「重要10項目」（2）

指示6：必要な予算や人材など資源の確保

指示7：自組織で対応する部分と他組織に委託する部分の、適切な切り分け

指示8：情報共有活動に参加し、最新の状況を自社の対策に反映。また情報共有活動に貢献

指示9：CSIRTの整備や、初動対応マニュアルの策定

指示10：被害発覚後の通知先や開示が必要な情報項目の整理。経営者によるスムーズな説明

サイバー・インシデントの特性

① 実行者の特定困難性：匿名化手段（TOR＝The Onion　Router ）や　ボット化・踏み台化（パソコンやサーバが乗っ取られ、指令サーバに支配される）などにより、誰が本当の実行者かの特定が困難
② 被害の潜在性（ステルス性）：ウイルス感染や、不正アクセスによる情報の窃取あるいは乗っ取りにも、痕跡を残さないので、被害者も気づかない
③　インシデントから攻撃までの連続性・越境性：偶発的インシデント、いたずら、営利目的、攻撃、テロ、武力攻撃の準備（インテリジェンス）までが、連続的に展開され区分が難しい上、容易に国境を越えてしまう
④ 責任の分散：後述のVarianの公式に示されるように、特定少数の担当者が気を付ければ済むことではなく、ほぼ全員が何らかの責任を分担せざるを得ないため、対策が立てにくく、実効性も担保しにくい
⑤ ICTの依存度と防御能力の反比例関係：上記を反映して、北朝鮮のようなICT依存度が低く、攻撃力だけを高めた国が優位に立ち、先進国はほぼ劣位になる

Varian の公式

セキュリティを担保するのは、3つの側面がある

- best shot：スーパー技術者が解決する（スーパー技術者しか解決できない）
- weakest point：一番弱いところが狙われ、そこから逐次的に侵入される
- total effort：bot-net のtake down など、みんなでやらなければならない面がある

（Source）Hal Varian [2004] ‘System Reliability and Free Riding’, in L. Jean Camp and Stephen Lewis (eds.) “Economics of Information Security” Kluwer

防御を難しくする7つの非対称

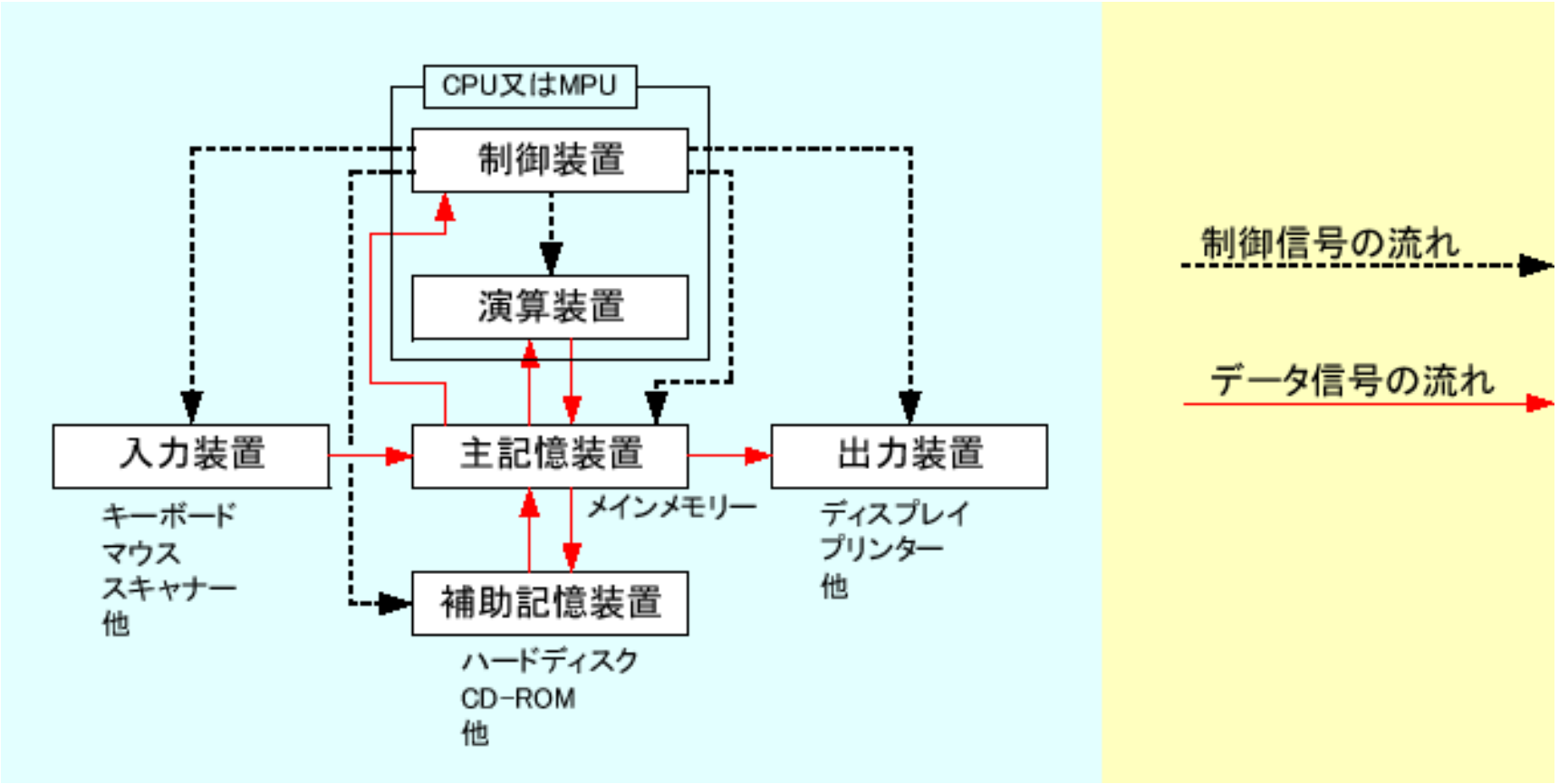
以下のいずれにおいても、攻撃側が優位

(1) 一点突破 対 全面防御、
(2) 簡単に手に入る攻撃ソフト 対 合法の事後対応、
(3) ゲリラ攻撃 対 正規軍（しかもタテ割り）、
(4) 緩やかな国際連携 対 国内組織、
(5) 多数の予備軍 対 少数精鋭、
(6) （一部国家の）暗黙の援助 対 国際秩序遵守
(7) （C&C方式なら）分散計算資源対 （セキュアな環境の）有限資源

サイバー対策は誰の役割か？

- 従来は専門家の仕事だと思われてきた：CIOやCISO
- また、民間主導で十分と思われてきた：ISMSやPマークなどのマネジメント・システムが中心
- しかし、前記の非対称性や（一部の）国家の関与が疑われ、攻撃対象に重要インフラ企業や防衛装備品のベンダーが含まれてきたころから、ナショナル・セキュリティにも関わるテーマだと意識されるようになった
- またアメリカでは、企業のリスク対策の一種だとして、取締役の責任が論ぜられるようになった

企業を、巨大な情報処理装置と見る



http://akita-nct.jp/yamamoto/lecture/2006/1E/31st/html/node2.html

Floridiがいう” Inforg = Information Organism“ に近い発想

すると、情報管理は取締役の役割

- 財務報告を操作すると、投資家等の利害関係者の利益を害することは明らか
- アメリカでは Caremark 判決（1996年、Delaware Court of Chancery）、日本では大和銀行事件判決（2000年大阪地裁、2001年に高裁で和解）が、取締役による「内部統制の構築」と「監視」の義務を認めた
- その後アメリカでは、いわゆる SOX 法が制定され、わが国では金融商品取引法と会社法において、「財務報告のための内部統制の構築」が、取締役の専決事項とされた
- しかし、財務報告以外の内部統制のあり方、とりわけ情報管理のあり方に関しては、ISO27000シリーズなどのソフトローに任されているのが現状

What's keeping you up at night?

- Directors: ① IT/Cybersecurity ② Operational risk ③ Succession planning ④ Crisis preparedness ⑤ Corporate reputation
- General Counsels: ① IT/Cybersecurity ② Regulatory compliance ③ Operational risk ④ Corporate reputation ⑤ Crisis preparedness

(Source) Law in the Boardroom Survey 2015, conducted jointly by FTI Consulting and *Corporate Board Member*

「有価証券報告書の調査」の主な結果

- 開示企業数は、平成21年度の52%（116社）から平成25年度の60%（136社）へと増加。
- 業種別では、通信、銀行、証券、保険、小売業、石油、造船、電力、ガス等の14業種が100%（合計51社）。
- 繊維、パルプ・紙、鉄鋼等の4業種は0%（合計14社）。
- 素材産業全体（64社）では開示割合が32.8%と低く、原材料費や為替の影響等のリスクと比べ、サイバーセキュリティリスクの認識が相対的に低いと考えられる。
- サイバーセキュリティリスクの記載文書が5年間同一の企業（65社）には、その記載の仕方が包括的で意味が広く捉えられる（想定インシデント・被害が具体的でない）ものが多かった。
- 自社で発生したサイバーセキュリティインシデントを記載している企業は調査対象企業中4社と少なかった。

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		

「海外文献調査」の主な結果（米国）

- 米国企業のForm 10-Kに記載するリスク要因については連邦規則（Regulation S-K Item503(c)）にて規定されており、どの企業にもあてはまるような一般的な記述ではなく、当該企業特有の内容について、具体的に分かり易く説明するよう要求されている。

- また、サイバーセキュリティリスク開示に関するガイダンスとしては、米国証券取引委員会（SEC）企業財務局から2011年10月に発行された「CF Disclosure Guidance: Topic No. 2 Cybersecurity」（CFDG: Topic No.2）がある。同文書は、上場企業がサイバーセキュリティについて、自社特有の事実と状況を考慮しつつ、どのような場合に何を開示すべきかを判断する助けとなるガイダンスである。

- 上記に基づき、米国企業においては、サイバーセキュリティに関する自社特有の事実・状況に照らしたリスクや想定被害について詳しく開示している傾向があり、被害事例を開示する企業も見られる。

- なお、証券法は、詳細な開示によって当該企業がサイバーセキュリティ上の危険に晒されるような場合にまで開示を求めるものではないとしている。

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

経営者の理解度
（本人の評価と他人の評価）

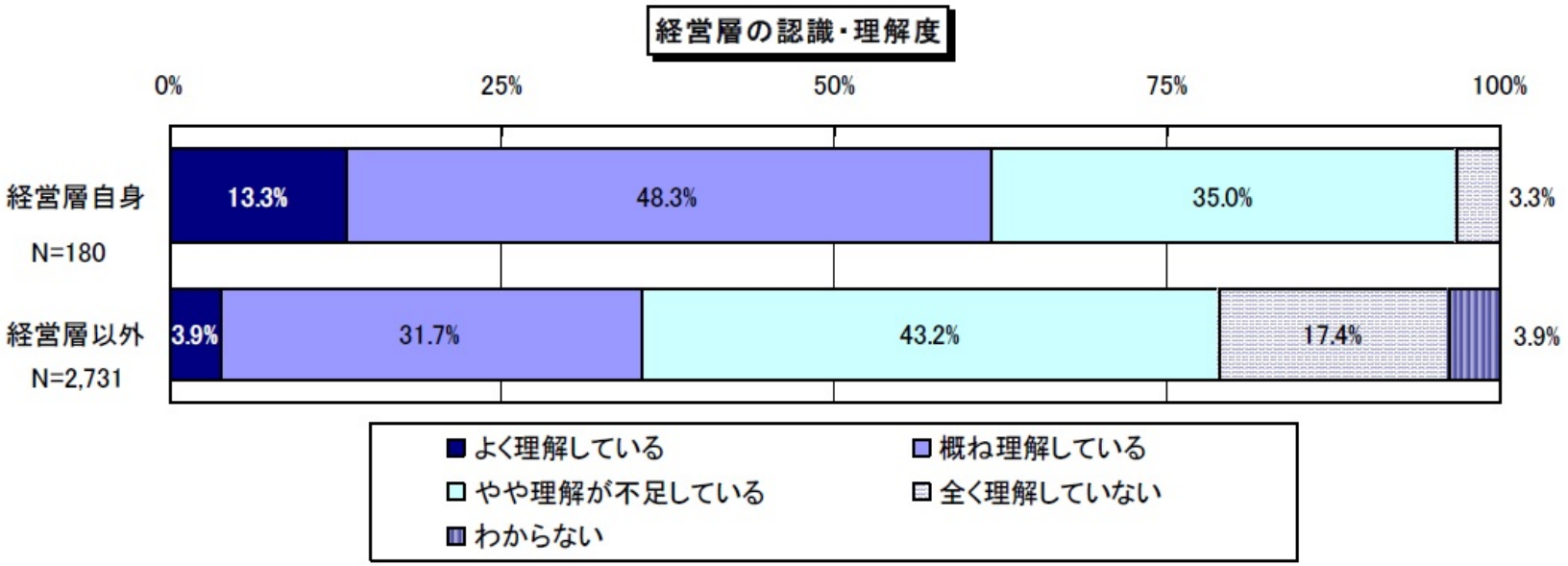


図　２－４７　経営層の認識・理解度［Q3－17］［Q3－19］

（出典）IPA「情報セキュリティの人材育成に関する基礎調査」2014年4月