2019/03 JSSM公開討論会

中小企業経営者のための サイバーセキュリティ・リスクモデル

JSSM 情報セキュリティ会計研究会
大木榮二郎

1

AGENDA

1. 検討の背景
2. 目的
3. 検討手法
   - A) 「企業価値に基づくサイバーセキュリティ・リスクモデル」を基礎
   - B) 中小企業の事業ミニマムモデルを構築とサイバー率 α
   - C) ターゲット率 β
   - D) 保護率 γ に簡易診断の活用
   - E) 新たなリスク表現チャートの採用
4. 今後の取り組み予定

2

1. 検討の背景

- 昨年の論文"経営者のための「企業価値に基づくサイバーセキュリティ・リスクモデル」の提案"の内容を発展させたい。
  - 大木榮二郎・田村仁一・清水恵子・杉浦昌・菊地正人・那須浩修・常川直樹・冨士浩一、『経営者のための「企業価値に基づくサイバーセキュリティ・リスクモデル」の提案』、日本セキュリティ・マネジメント学会誌、32、No.1、pp.16-32(2018)
  - 大木榮二郎, 田村仁一, 清水恵子, 佐野智己, 芹沢大地、『経営に役立つ情報セキュリティ会計の提案』、日本セキュリティ・マネジメント学会誌、25、No.2、pp.15-41(2011)
- 我が国産業にとって、中小企業のセキュリティ対策を強化することが極めて重要である。
- IPAの「中小企業の情報セキュリティ対策ガイドライン」を改訂中であるが、中小企業経営者にとって理解しやすく実感できるリスクモデルが提示できないことが課題である。

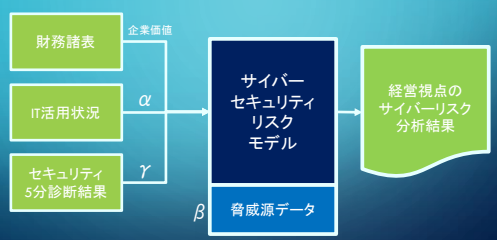
3

2. 目的

- 企業を取り巻く環境や、企業内の資産や業務を簡素化した企業モデルを作成し、サイバーセキュリティ・リスクモデルを適用することで、簡易リスクモデルを構成し、経営者の役に立つことを目的とする。
- 中小企業の経営者にとって、簡易モデルをもとに、自社の実情に沿って少し手を加えることにより、経営視点から実用的なリスクモデルが手に入るようにする。
- 「中小企業の情報セキュリティ対策ガイドライン」と連携させ、セキュリティ対策に対する中小企業経営者の認識を改めることに貢献する。

4

目指すリスクモデルの活用方式



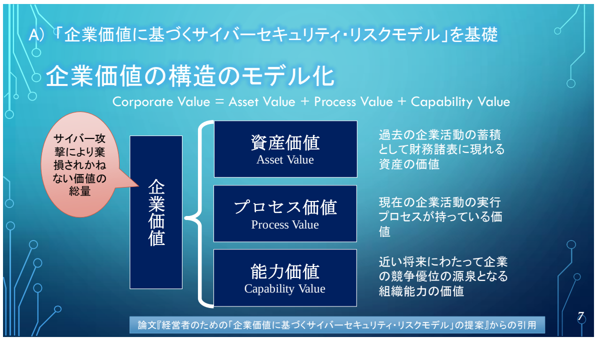
5

3. 検討手法

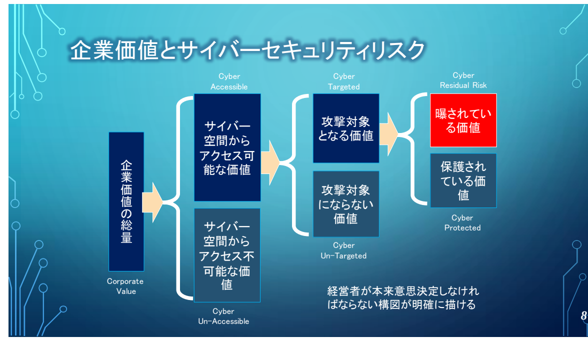
- 企業価値の構成要素を大胆に簡略化
- フェルミ推定　Physicist Enrico Fermi

  The Fermi Rule: Better be Approximately Right than Precisely Wrong
  - サイバー率α　企業価値構成要素のIT活用度から推定
  - ターゲット率β　サイバー攻撃の構造モデルと測定値から推定
  - 保護率γ　情報セキュリティ対策自社診断から推定
- 直観的に理解しやすい表現形式を検討
- 企業の協力を得て検証していきたい

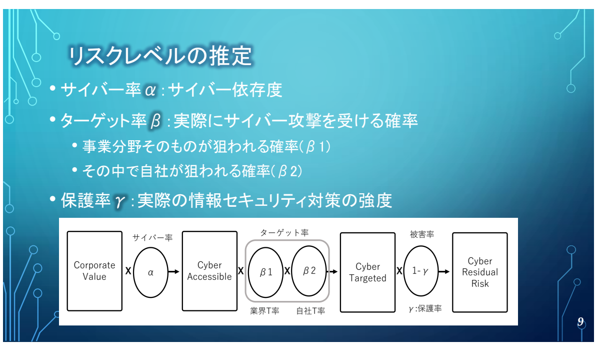
6


A)「企業価値に基づくサイバーセキュリティ・リスクモデル」を基礎
企業価値の構造のモデル化
Corporate Value = Asset Value + Process Value + Capability Value
サイバー攻撃により棄損されかねない価値の総量
企業価値
資産価値
Asset Value
過去の企業活動の蓄積として財務諸表に現れる資産の価値
プロセス価値
Process Value
現在の企業活動の実行プロセスが持っている価値
能力価値
Capability Value
近い将来にわたって企業の競争優位の源泉となる組織能力の価値
論文『経営者のための「企業価値に基づくサイバーセキュリティ・リスクモデル」の提案』からの引用
7

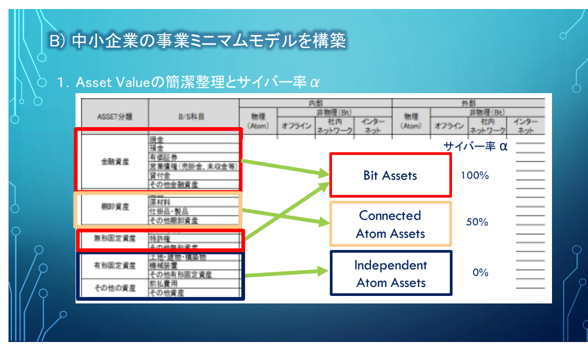
7


企業価値とサイバーセキュリティリスク
企業価値の総量
Corporate Value
Cyber Accessible
サイバー空間からアクセス可能な価値
サイバー空間からアクセス不可能な価値
Cyber Un-Accessible
Cyber Targeted
攻撃対象となる価値
攻撃対象にならない価値
Cyber Un-Targeted
Cyber Residual Risk
曝されている価値
保護されている価値
Cyber Protected
経営者が本来意思決定しなければならない構図が明確に描ける
8

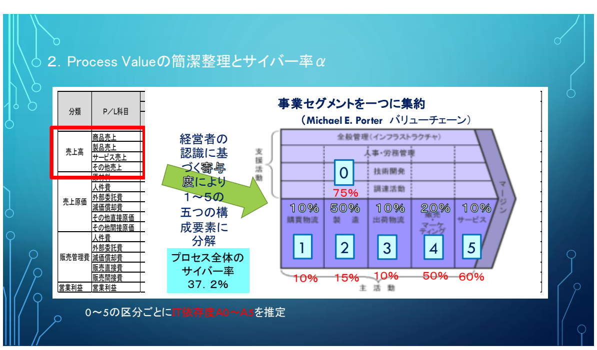
8


リスクレベルの推定
• サイバー率 α : サイバー依存度
• ターゲット率 β : 実際にサイバー攻撃を受ける確率
• 事業分野そのものが狙われる確率(β1)
• その中で自社が狙われる確率(β2)
• 保護率 γ : 実際の情報セキュリティ対策の強度
Corporate Value
サイバー率
α
Cyber Accessible
ターゲット率
β1
β2
業界T率
自社T率
Cyber Targeted
被害率
1-γ
γ:保護率
Cyber Residual Risk
9

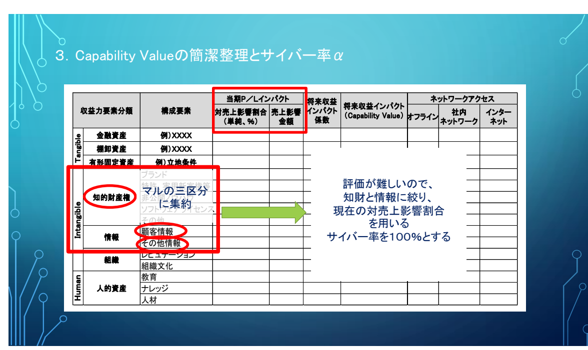
9


B) 中小企業の事業ミニマムモデルを構築
1. Asset Valueの簡潔整理とサイバー率 α
ASSET分類
B/S科目
内部
外部
物理 (Atom)
非物理(Bit)
オフライン
社内ネットワーク
インターネット
金融資産
現金
預金
有価証券
営業債権(売掛金、未収金等)
貸付金
その他金融資産
棚卸資産
原材料
仕掛品・製品
その他棚卸資産
無形固定資産
特許権
有形固定資産
土地・建物・構築物
機械装置
その他有形固定資産
その他の資産
前払費用
その他資産
サイバー率 α
Bit Assets
100%
Connected Atom Assets
50%
Independent Atom Assets
0%

10


2. Process Valueの簡潔整理とサイバー率 α
分類
P/L科目
売上高
商品売上
製品売上
サービス売上
その他売上
売上原価
人件費
外部委託費
減価償却費
その他直接原価
その他間接原価
販売管理費
人件費
外部委託費
減価償却費
販売直接費
販売間接費
営業利益
営業利益
経営者の認識に基づく寄与度により1～5の五つの構成要素に分解
プロセス全体のサイバー率 37. 2%
事業セグメントを一つに集約
(Michael E. Porter バリューチェーン)
全般管理(インフラストラクチャ)
人事・労務管理
技術開発
調達活動
支援活動
0
75%
10%
購買物流
50%
製造
10%
出荷物流
20%
販売・マーケティング
10%
サービス
1
2
3
4
5
10%
15%
10%
50%
60%
主活動
マージン
0～5の区分ごとにIT依存度A0～A5を推定

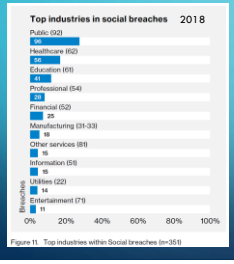
11


3. Capability Valueの簡潔整理とサイバー率 α
収益力要素分類
構成要素
当期P/Lインパクト
対売上影響割合 (単純、%)
売上影響金額
将来収益インパクト係数
将来収益インパクト (Capability Value)
ネットワークアクセス
オフライン
社内ネットワーク
インターネット
Tangible
金融資産
例)XXXX
棚卸資産
例)XXXX
有形固定資産
例)立地条件
Intangible
知的財産権
ブランド
その他
マルの三区分に集約
情報
顧客情報
その他情報
組織
組織文化
Human
人的資産
教育
ナレッジ
人材
評価が難しいので、
知財と情報に絞り、
現在の対売上影響割合
を用いる
サイバー率を100%とする

12

C) ターゲット率 β

Verizon 等の業種別データの活用を検討



2017

Incidents / Breaches

	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	42,068	806	22,273	18,989	1,935	432	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	90	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,731	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,099	7,118	68	2	15	51
Total	42,068	806	22,273	18,989	1,935	432	278	1,224

Table 1: Number of security incidents by victim industry and organization size, 2016 dataset

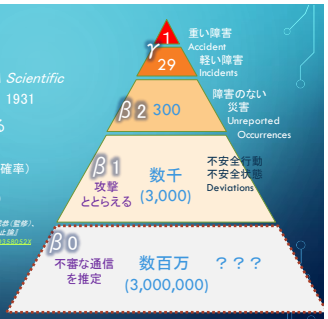
13

ハインリッヒの法則

- *"Industrial Accident Prevention, A Scientific Approach"*, Herbert W Heinrich、 1931
- 被害統計から攻撃頻度を推定する
- □ ハインリッヒの産業災害防止論:
  リスク＝（潜在危険性が事故となる確率）
  ×（事故に遭遇する可能性）
  ×（事故による被害の大きさ）

H. W. ハインリッヒ, D. ピーターセン, N. ルース(著)/井上威恭(監修), (財)総合安全工学研究所(訳)『ハインリッヒ産業災害防止論』海文堂出版(株) 1987年(昭和62年)9月 5版 ISBN 4303158052X

=＞被害の背景の構造としては使えるか



14

「脅威は遍在する」ことをベースに推定

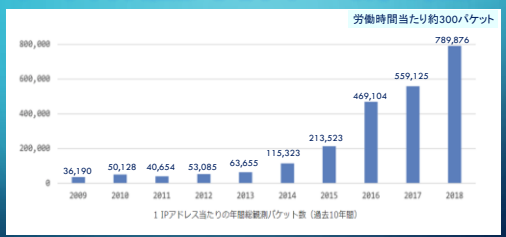
ターゲット率 β を次のように構成する

β0 × β1 × β2

β0	β1	β2
世の中全体の攻撃密度指標	業態により攻撃対象となる確率	自社が攻撃に遭遇する確率

15

β0 ダークネット観測によるサイバー攻撃の状況

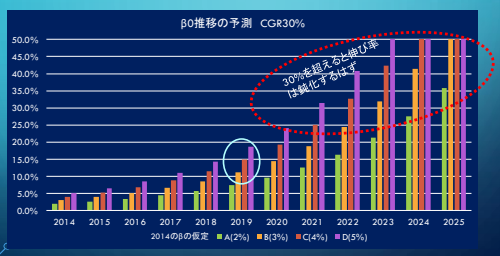


①成長曲線に当てはめて現状を推定するか（誤差大となりそう）
②世界的な迷惑メールの割合は55%程度(迷惑メール白書2018)

NICTER 観測レポート2018
国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所サイバーセキュリティ研究室

16

β0はCGR=30%で増加が続きいずれ50%に収束すると仮定すれば、不正通信の割合は2019 10～20% 程度か？



17

β1 VERIZON データ漏洩/侵害調査報告書

- 業界別の被害(漏洩、侵害)実態がGlobal 規模で調査されている
- 10年以上にわたって継続的にレポートが出されている
- 年ごとにまとめ方が多少異なる
- 統計的に比較できるデータは開示されていない
- 活用には注意が必要
- 業種別の被害実態について有用な情報が得られる

=＞業種を直接区分に用いるのは難しい

Incident's / Breaches

業界	2015	合計	中小規模の企業・組織	大規模の企業・組織	不明
ホテル業 (72)		140	0	80	60
管理サービス業 (56)		164	0	1	163
農業 (11)		0	0	0	0
建設業 (23)		0	0	0	0
教育サービス業 (61)		10	0	0	10
芸術/娯楽業 (71)		1	0	0	1
金融業 (52)		184	1	17	166
医療業 (62)		17	3	1	13
情報産業 (51)		72	16	8	48
マネジメントサービス (55)		2	0	1	1
製造業 (31-33)		157	2	22	133
鉱業 (21)		3	0	0	3
その他のサービス業 (81)		11	3	0	8
専門サービス業 (54)		161	4	1	156
公的機関 (92)		435	0	245	190
不動産業 (53)		0	0	0	0
小売業 (44-45)		207	1	3	203
娯楽/運輸業 (42)		6	6	0	0
運輸業 (48-49)		3	0	0	3
公益事業 (22)		2	0	0	2
不明		860	0	0	860
合計		2,435	36	379	2,020

18

背後に想定される攻撃者の狙いによるターゲット率の推定に方針を変更

	業界	インシデントの件数　合計				
		2014	2015	2016	2017	2018
1	ホテル業（72）	212	368	362	215	368
	管理サービス業（56）	16	205	44	42	33
	農業（11）	4	2	4	11	5
	建設業（23）	4	3	9	6	23
2	教育サービス業（61）	33	165	254	455	292
	芸術/娯楽業（71）	20	27	2,707	5,534	7,188
3	金融業（52）	856	642	1,368	998	598
4	医療業（62）	26	234	166	458	750
5	情報産業（51）	1,132	1,496	1,028	717	1,040
	マネジメントサービス（55）	10	4	1	8	2
6	製造業（31–33）	251	525	171	620	536
	鉱業（21）	11	22	11	6	26
	その他のサービス業（81）	27	263	17	69	62
7	専門サービス業（54）	360	347	916	3,016	540
	公的機関（92）	47,479	50,315	47,237	21,239	22,788
	不動産業（53）	8	14	11	13	31
8	小売業（44–45）	467	523	159	326	317
	貿易/通商業（42）	4	14	15	20	31
	運輸業（48–49）	27	44	31	63	59
	公益事業（22）	166	73	24	32	46
	不明	12,324	24,504	9,453	8,220	18,573
	合計	63,437	79,790	64,199	42,068	53,308

- データの整合する2014～2018を取り上げ、その5年の平均をとる。
- 中小企業向けに有用な業種を選択する
  - 調査数の少ない業種を除く
  - 業種説明の記述がない業種を除く
  - 公的機関と不明を除く
- 残りの8業種を対象として、背後にある攻撃者の狙いを推定する

19

攻撃者の狙い（窃取目的の情報の種別）と自社の情報重要度により、攻撃対象になる確率を推定する

	業界	2014~2918の平均インシデント数	構成比	情報窃取目的 支払情報 p	個人情報 q	医療情報 r	認証情報 s	技術情報 t	
1	ホテル業（72）	305	6.5%	9	1				9p+q=65
5	教育サービス業（61）	240	5.1%		6	1		3	6q+r+3t=51
7	金融業（52）	892	19.1%	5	4		1		5p+4q+s=191
8	医療業（62）	327	7.0%	1	2	7			p+2q+7r=70
9	情報産業（51）	1,083	23.2%	1	4		4	1	p+4q+4s+1t=232
11	製造業（31–33）	421	9.0%	3				7	3p+7t=90
14	専門サービス業（54）	1,036	22.2%		5		2	3	5q+2s+3t=222
17	小売業（44–45）	358	7.7%	7	2		1		7p+2q+s=77
22	合計	4,661	100.0%						

p+q+r+s+t=100 の関係により、独立変数は4、式は8となる

業種別記述より、攻撃者が狙った情報の相対構成比に展開

最小二乗法により、この関係を満たすに一番近い（p,q,r,s,t）を見つける

20

β2　自社が攻撃に遭遇する確率の推定

- 価値要素ごとに、攻撃に遭遇しやすい仮説を立てて質問集を構成する

QA1　預貯金や有価証券はネット経由で取引しているか　Yes/No

QA2　製品や部品の出庫はネット経由で管理しているか　Yes/No

QP1　社内の連絡にも電子メールを使っている　Yes/No　p0 %
QP2　原材料の取引先への発注方法の割合(%)　電話/Fax　オンライン p1　電子メール p2　郵送　合計100%
QP3　製造ラインの自動化割合　p11 %
QP4　製品の出荷指示の方法　電話/Fax　オンライン p3　電子メール p4　合計100%
QP5　顧客からの受注受付の方法　電話/Fax　オンライン p5　電子メール p6　郵送　合計100%
QP6　顧客からのサービス業務受付の方法　電話/Fax　オンライン p7　電子メール p8　郵送　合計100%

QC1　知識やノウハウなどをデータベース化しているか　Yes/No
QC2　顧客情報に機微な情報を含んでいるか　Yes/No

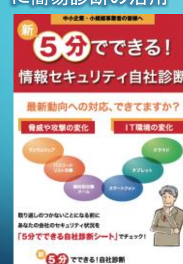
Q01　ネット販売が売上に占める割合　p9 %
Q02　世界的企業のサプライチェーンでの売上が占める割合　p10 %

21

D）保護率 γ に簡易診断の活用

中小企業向けの情報セキュリティ対策ガイドラインを改訂中

この診断ツールの内容は実質的に変わらない



22

保護率 γ を5分診断の結果のスコアから推定

入門レベルの対策ができていれば、攻撃の8割には対抗できると考える

γ =0.8*スコア

回答結果をもとに採点し、対策を検討しましょう

100点満点だった方	入門レベルのセキュリティ対策はもう完璧です。ステップアップを検討しましょう。	「中小企業の情報セキュリティ対策ガイドライン」4.本格的に取り組むを参照して、情報セキュリティ対策の強化に取り組みましょう。
70～99点だった方	ほぼ、出来ていますが、部分的に対策が不十分な点があるようです。	小さな隙間から情報が漏えいすることもあります。100点満点を目指しつつ、「中小企業の情報セキュリティ対策ガイドライン」を参考に本格的に取り組みましょう。
50～69点だった方	対策が行き届いていないところが目立ちます。	点数が低かった項目について、「5分でできる！情報セキュリティ自社診断」の解説編を参考にして、対策を施しましょう。
49点以下だった方	いつ情報流出などの事故が起きても不思議ではありません。	「5分でできる！情報セキュリティ自社診断パンフレット」や「対策のしおり」「映像で知る情報セキュリティ」を利用して、分からなかった部分や点数が低かった項目を確認し、対策を施しましょう。

これより上は、「情報セキュリティ対策ベンチマーク」の使用を検討したい。

23

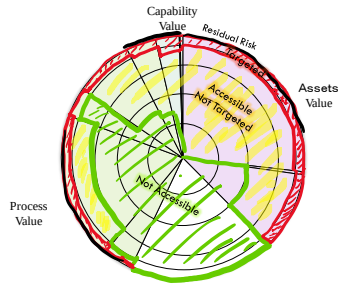
E）新たなリスク表現チャートの採用

価値構成		価値額	α	Cyber Accessible	β0	β1	β2	β 1*2*3	Cyber Targeted	γ	Cyber Residual Risk
Assets	金融資産										
	無形固定資産										
	棚卸資産										
	その他資産										
	小計										
Process	[1]購買物流										
	[2]製造										
	[3]出荷物流										
	[4]販売・マーケティング										
	[5]サービス										
	小計										
Capability	知的財産										
	顧客情報										
	その他情報										
	小計										
合計											

24

CYBER RISK APPLE CHART

リスクマップを円グラフで示し外からの脅威の状況を表す



25

4. 今後の取り組み予定

- β0、β1 推定根拠の補強
- β2 推定に用いる質問リスト方式の改善と的確性の検証
- 経営者とのパラメータの納得性の検証
- 解説を加えて、Excel で Tool "Cyber Risk Tool 2019" に仕上げて発表したい
- 新たなメンバーの参加を歓迎します。
- 実証に参加いただける企業、団体を歓迎します。

26

Thank you.

Eijiroh Ohki

27