RO-006

オフィス空間における場のセキュリティを考慮したリスクアセスメント

Risk Assessment with Various Security Factors in Office Environment

米田 翔一* 谷本 茂明* 佐藤 周行** 金井 敦***
Shoichi Yoneda* Shigeaki Tanimoto* Hiroyuki Sato** Atsushi Kanai***

1. まえがき

近年，インターネットやモバイル通信は社会基盤の重要な要素として急速に発展している．一方，これらの普及に比例して情報セキュリティに関するインシデントが増加している．平成 25 年中のサイバー犯罪の検挙件数は 8,113 件で，不正アクセス禁止法違反は現在も増加傾向にある [1]．上記のように情報社会には様々な脅威があり，これらの脅威から情報資産を守るために然るべき対処を取らなければならない．このような情報セキュリティの対処方法を定め，構築及び運用などの活動を一貫して管理することを情報セキュリティマネジメントと呼ぶ [2]-[3]．現状，このマネジメントについて積極的に取り組んでいる企業が増加しており，その中でも特にプライバシーマークや ISMS（情報セキュリティマネジメントシステム，ISO/IEC 27001）を取得している企業が次第に増えてきているが [4]-[5]，サイバー犯罪件数を見る限り現在の情報社会はまだ十分に安全とは言えない．

一方，クラウドの進展に伴い，データセンターが数多く構築されているが，このようなデータセンターでは，厳格な入退室管理が行われている．このように，情報セキュリティに加え物理セキュリティも加味したセキュリティマネジメントが重要になってきている [6]-[9]．

一般に，守るべき情報資産の価値や脅威は，TPO（時間，場所，機会）条件に応じて常に変化する．このような場合を考慮すると，従来の情報セキュリティに加え，物理セキュリティも加味した総合的なセキュリティの考え方が重要となってくる．しかし，これまでにこのような総合的なセキュリティに言及した研究は十分では無い．

本論文では，企業のオフィス空間を対象に，これら情報セキュリティに物理セキュリティを加味した総合的なセキュリティについて述べる．具体的には，オフィス空間を対象に，情報セキュリティと物理セキュリティが作用する場のセキュリティとして捉え，この場のセキュリティにおけるリスクアセスメントについて述べる．オフィス空間における場のセキュリティを考慮したリスクアセスメントとして，情報セキュリティの観点に物理セキュリティの観点を加えたリスク分析を行い，リスク要因を抽出する．次に，これらのリスク要因に対し，リスクマトリクス手法に基づきリスク対策案を提案し，情報セキュリティに物理セキュリティを加味した総合的なセキュリティ対策について示す．

* 千葉工業大学 (Chiba Institute of Technology)
** 東京大学 (The University of Tokyo)
*** 法政大学 (Hosei University)

2. オフィス空間における場のセキュリティ

2.1 物理セキュリティ

一般に，オフィスにおける情報資産を守るために機密性，完全性，可用性を維持しなければならない．これには，暗号，認証などの情報セキュリティの技術以外に，警備員や監視カメラの導入，施錠の実施など運用やハード面，即ち，物理セキュリティが欠かせない．物理セキュリティは，監視カメラ，人感センサ，測位センサ，RFID などのセンサ技術の進展により，物理的な認証技術を中心に，より複雑で堅固なものに進歩している．

2.2 情報セキュリティ

情報セキュリティでは，一般に，ファイアウォールやアンチウィルスソフトなどによりインターネットなどの外部の脅威から情報資産を守っている．これに対し，例えば，個人情報漏えい事件の約 8 割は内部犯によるものであると言われており [10]，外部からの進入を防ぐだけでは十分ではない．例えば，ISMS などによるポリシーに基づく情報セキュリティマネジメントも加味する必要がある．

2.3 場のセキュリティ

上記のように，オフィスでは，物理面，情報面と様々なセキュリティインシデントが顕在化している．さらに，守るべき情報資産の価値や脅威は，TPO 条件に応じて常に変化するものである．これらについて，個々に対処するのではなく，連携して総合的に対処することがより効率的であると考えられる．

本論文では，オフィス空間を対象に，情報セキュリティと物理セキュリティを統合化した，場のセキュリティを提案する．具体的には，場のセキュリティに対し，総合的なセキュリティ対策の現状分析として，そのリスクアセスメントについて述べる．

3. オフィス空間における場のセキュリティ

オフィス空間における場のセキュリティを検討するにあたり，現状分析を行う必要がある．ここでは，オフィス空間における場のセキュリティとして，そのリスク要因を抽出する．

3.1 リスク要因の抽出

リスク要因の抽出には，リスクマネジメントの代表的な手法である RBS（Risk Breakdown Structure）手法を用い [11]，27 項目を抽出した．表 1 にその結果を示す．同表では，オフィス空間における場のセキュリティとしてのリスク要因を階層的な観点[12] から，物理セキュリティと情報セキュリティにまず分解し，次に物理セキュリティは人為的か否かとして分解した．さらに人為的の場合は，意図的か否かとして分解した．情報セキュリティの場合は，インターネットなどが，人工物でかつ実体を持たないため，非人為的，すなわち自然現象などといったリスクが存在しないとして，人為的か否かの階層を省略し，意図的か否かへと分解した．

表 1　RBS 手法に基づく場のセキュリティにおけるリスク要因抽出結果

分類			リスク要因	リスク要因詳細
1. 物理セキュリティ	1.1 人為的	1.1.1 意図的	1.1.1.1 侵入	許可なしにセキュリティ空間に入られてしまう．一般的に施錠などの抑制システムがある．発生した場合，自由に活動されてしまうため，影響度は高い．
			1.1.1.2 盗難	書類や機材などの物品を奪われてしまう．法律として禁止され，抑制されている．機材を奪われると，情報漏えいだけでなく業務の続行にも影響がある．
			1.1.1.3 聞き出し	上司などを装って機密情報を聞き出されてしまう．法律として禁止され，抑制されている．情報漏えいの発生など，影響度は大きい．
			1.1.1.4 放火	社屋に火をつけられてしまう．法律として禁止され，抑制されている．社屋全焼の可能性など影響度は高い．
			1.1.1.5 破壊	機材を壊したり，回線を切断されてしまう．法律として禁止され，抑制されている．業務続行が難しくなる可能性が高く，影響度は高い．
			1.1.1.6 覗き見	PC の画面などを背後から見られてしまう．一般的に利用されている抑制システムはない．業務続行には影響はなく，見た記憶に頼るため影響はやや低い．
			1.1.1.7 聞き耳	許可されてない者に会話を聞かれてしまう．一般的に利用されている抑制システムはない．業務続行に影響はなく，聞いた記憶に頼るため影響はやや低い．
			1.1.1.8 内部犯行	許可された人間に犯行を行われてしまう．一般的に身元の確認などの対策は行っているため，発生頻度は低い．情報漏えいの発生など，影響度は大きい．
		1.1.2 非意図的	1.1.2.1 書置き	メモを書いて机の上などに残してしまう．一般的に利用されている抑制システムはない．置いてあるだけではまだ問題がないため，影響度は低いとする．
			1.1.2.2 火の不始末	火器を使用したあと，消火し忘れてしまう．一般的に，厳格に管理され抑制されている．火災に繋がる可能性があり，影響度は高い．
			1.1.2.3 破壊	不注意で機材を落とすなどで壊してしまう．通常使用において機材が壊れることは少ない．業務続行が難しくなるなど，影響度は高い．
			1.1.2.4 紛失	使用していた機材やデータを失くしてしまう．一般的に利用されている抑制システムはない．情報漏えいなど，影響度は大きい．
			1.1.2.5 持ち出し	データや書類などを持って社外に出てしまう．一般的に利用されている抑制システムはない．持ち出しただけではまだ問題がないため，影響度は小さいとする．
			1.1.2.6 持ち込み	許可されていない機材を持ち込んで作業してしまう．一般的に厳格に管理され，抑制されている．ウィルスの感染や情報漏えいの発生など，影響度は高い．
	1.2 非人為的		1.2.1 故障	機材などが故障して使えなくなってしまう．一般的に製造時の品質管理などの抑制システムがある．誤動作や業務の停止など，影響度は高い．
			1.2.2 災害	自然災害に見舞われてしまう．一般的に自然災害の被害に遭う可能性は低い．業務続行が難しくなるなど，影響度は高い．
2. 情報セキュリティ	2.1 意図的		2.1.1 ウィルスの感染	コンピュータウィルスに感染してしまう．一般的にウィルス対策ソフト導入などの抑制システムがある．ウィルスによる被害は多岐に渡り，影響度は高い．
			2.1.2 不正アクセス	コンピュータに許可なくアクセスされてしまう．一般的にファイアウォール導入などの抑制システムがある．情報漏えいの発生など，影響度は高い．
			2.1.3 盗聴	データ通信を傍受されてしまう．一般的に暗号化などの抑制システムがある．情報漏えいの発生など，影響度は高い．
			2.1.4 なりすまし	ID などを取得して，不正に権限を得られてしまう．法律として禁止され，抑制されている．情報漏えいの発生など，影響度は高い．
			2.1.5 DoS 攻撃	コンピュータに大量のデータを送りつけ，停止させられてしまう．一般的にファイアウォール導入などの抑制システムがある．業務が停止するなど，影響度は高い．
			2.1.6 改ざん	データを許可なく変更されてしまう．一般的にアクセス管理などの抑制システムがある．重要文書のデータ改ざんは業務に混乱を招き，影響度は高い．
			2.1.7 否認	執り行われた契約などを，後からやっていないと否定されてしまう．一般的に，身元のわかる契約で否認することは少ない．業務の混乱など，影響度は高い
			2.1.8 不正コピー	ソフトなどを許可されてない範囲で複製されてしまう．法律として禁止され，抑制されている．信用の失墜など，影響度は高い．
			2.1.9 フィッシング	偽サイトに個人情報などを入力させることによって盗み取られてしまう．法律として禁止され，抑制されている．情報漏えいの発生など，影響度は高い．
	2.2 非意図的		2.2.1 誤操作	システムを誤って操作してしまう．一般的に利用されている抑制システムはない．情報漏えいの発生や重要データの消失など，影響度は大きい．
			2.2.2 バグ	システムの不具合により意図せぬ動作をしてしまう．一般的に品質管理やテストなどで抑制されている．発生する被害は多岐に渡り，影響度は大きい．

3.2 リスク分析

リスク分析手法は，定性的な評価をする観点からリスクマトリクス手法を用いる [11]．これは，図 1 に示すように，リスクの発生頻度，影響度の高低により，回避，低減，保有，転嫁の 4 種類に分類し，その対策を策定するものである．

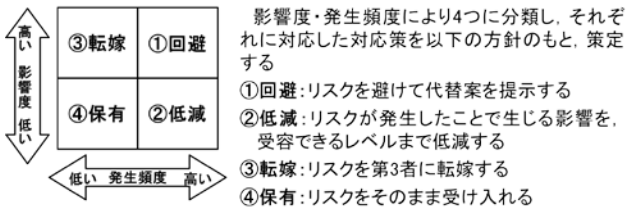

図 1 リスクマトリクス手法

3.3 リスクの分析結果

表 1 に示す，場のセキュリティにおける 27 のリスク要因に対し，図 1 に示すリスクマトリクス手法を用いて，詳細に分析を行った．結果を表 2 に示す．

表 2　場のセキュリティのリスク要因に対する分析結果

分類	リスク要因	頻度	影響	対応策
1. 物理セキュリティ	1.1.1.1 侵入	低	高	転嫁
	1.1.1.2 盗難	低	高	転嫁
	1.1.1.6 聞き出し	低	高	転嫁
	1.1.1.3 放火	低	高	転嫁
	1.1.1.4 破壊	低	高	転嫁
	1.1.1.5 覗き見	高	低	低減
	1.1.1.7 聞き耳	高	低	低減
	1.1.1.8 内部犯行	低	高	転嫁
	1.1.2.1 書置き	高	低	低減
	1.1.2.2 火の不始末	低	高	転嫁
	1.1.2.3 破壊	低	高	転嫁
	1.1.2.4 紛失	高	高	回避
	1.1.2.5 持ち出し	高	低	低減
	1.1.2.6 持ち込み	低	高	転嫁
	1.2.1 故障	低	高	転嫁
	1.2.2 災害	低	高	転嫁
2. 情報セキュリティ	2.1.1 ウィルスの感染	低	高	転嫁
	2.1.2 不正アクセス	低	高	転嫁
	2.1.3 盗聴	低	高	転嫁
	2.1.4 なりすまし	低	高	転嫁
	2.1.5 DoS 攻撃	低	高	転嫁
	2.1.6 改ざん	低	高	転嫁
	2.1.7 否認	低	高	転嫁
	2.1.8 不正コピー	低	高	転嫁
	2.1.9 フィッシング	低	高	転嫁
	2.2.1 誤操作	高	高	回避
	2.2.2 バグ	低	高	転嫁

表 2 より，場のセキュリティとしてのリスク要因に対する対応策では，図 1 の「転嫁」，すなわち，発生頻度は低いが，影響度が高いものが 27 項目中 21 項目と大半を占めることがわかった．次に，「低減」，すなわち，発生頻度は高いが，影響度が低いものが 4 項目であった．以下，発生頻度が高く，影響度も高い「回避」については 2 項目，発生頻度も 影響度も低い「保有」は 0 項目であった．

4. 場のセキュリティにおけるリスクアセスメント

4.1 リスクアセスメント結果

ここでは，表 2 の対応策分類の転嫁，低減，回避毎にリスクアセスメントした結果を以下に示す．

4.1.1 転嫁に分類されたリスク要因の対策案

転嫁に分類されたリスク要因は，図 1 の③転嫁に示すように，リスクを第 3 者に転嫁する方針で対策を検討した．結果を表 3 に示す．

表 3　転嫁に分類されたリスク要因のアセスメント結果

リスク要因	対策案	傾向
1.1.1.1 侵入	警備会社に委託するなどより強固な入退室管理システムを導入する	(a)管理強化
1.1.1.2 盗難	盗難保険に入る．外部にバックアップを用意する．	(b)業務停止の防止
1.1.1.3 聞き出し	クライアント証明書などを利用して確実に本人確認を行う	(a)管理強化
1.1.1.4 放火	火災保険に入る．外部にバックアップを用意する	(b)業務停止の防止
1.1.1.5 破壊	外部にバックアップを用意する	
1.1.1.8 内部犯行	雇用契約の内容を調整して法的処罰を与えられるようにする	(c)資産の流出防止
1.1.2.2 火の不始末	火災保険に入る．外部にバックアップを用意する	(b)業務停止の防止
1.1.2.3 破壊	外部にバックアップを用意する	
1.1.2.6 持ち込み	雇用契約の内容を調整して法的処罰を与えられるようにする	(c)資産の流出防止
1.2.1 故障	修理交換の保障制度を利用する	(b)業務停止の防止
1.2.2 災害	外部にバックアップを用意するなど，事業継続計画を立てる	
2.1.1 ウィルスの感染	ウィルス定義ファイルを常に更新しておく	(c)資産の流出防止
2.1.2 不正アクセス	アップデートを常に行い，脆弱性を解消しておく	
2.1.3 盗聴	アップデートを常に行い，脆弱性を解消しておく	
2.1.4 なりすまし	バイオメトリクスなど，強固な認証システムを導入する	
2.1.5 DoS 攻撃	アップデートを常に行い，脆弱性を解消しておく	(b)業務停止の防止
2.1.6 改ざん	アップデートを常に行い，脆弱性を解消しておく	
2.1.7 否認	電子公証システムなどを利用する	
2.1.8 不正コピー	不正コピー確認ツールなどを利用する	(a)管理強化
2.1.9 フィッシング	電子公証システムなどを利用する	(c)資産の流出防止
2.2.2 バグ	契約内容の調整を行う	(a)管理強化

4.1.2 低減に分類されたリスク要因の対策案

低減に分類されたリスク要因は，図 1 の②低減に示すように，リスクを，受容できるレベルまで低減する方針で対策を検討した．その結果を表 4 に示す．

表 4　低減に分類されたリスク要因のアセスメント結果

リスク要因	対策	傾向
1.1.1.6 覗き見	訪問者に画面を見せないようオフィスのポリシーを徹底する	(c)資産の流出防止
1.1.1.7 聞き耳	他者のいる場所での会話に気をつけるようオフィスのポリシーを徹底する	
1.1.2.1 書置き	機密情報の管理についてオフィスのポリシーを徹底する	
1.1.2.5 持ち出し	持ち出すデータの管理をオフィスのポリシーを徹底する	

4.1.3 回避に分類されたリスク要因の対策案

回避に分類されたリスク要因は，図 1 の①回避に示すように，リスクを避けて代替案を提示する方針で対策を検討した．その結果を表 5 に示す．

表 5　回避に分類されたリスク要因のアセスメント結果

リスク要因	対策	傾向
1.1.2.4 紛失	体系的な管理を行い，所定の場所から移動させない	(a)管理強化
2.2.1 誤操作	特に重要なシステムは複数人で操作する，指差し確認などを行う	

4.2 考察

表 3〜5 に示すリスク要因のアセスメント結果を基に考察する．

(1) 転嫁：対応策が転嫁に分類されたリスク要因は表 3 に示す結果となった．主に，資産の流出や業務の停止を防止する対策が有効である．具体的には，外部バックアップや証明書等の対策が有効であるが，これらは，一般に新たな費用が発生することになる．

今後，発生確率の低い要因に対して，どこまで対策をすれば良いのか，すなわち，影響度のレベルごとの対応，具体的には，費用対効果に関する定量的な検討が必要になってくると思われる．

(2) 低減：対応策が低減に分類されたリスク要因は表 4 に示す結果となった．いずれも資産の流出を防止する対策であり，具体的な対策案は，オフィスのポリシーに基づく社員教育によるものであるが，より確実な対策を行うために，システム的な対策案の検討も重要であると考えられる．

(3) 回避：対応策が回避に分類されたリスク要因は表 5 に示す結果となった．いずれのリスク要因も，非意図的に発生するもので，注意していても完全に避けることが難しいものが挙げられた．対策としては，ISMS などに基づく管理強化が重要である．

(4) 保有：対応策が保有に分類されたリスク要因は存在しなかった．セキュリティに関する内容のため，保有可能なリスク要因はなかったと考えられる．

5. おわりに

本論文では，企業のオフィス空間を対象に，情報セキュリティに物理セキュリティを加味した総合的なセキュリティについて述べた．オフィス空間を，情報セキュリティと物理セキュリティが作用する場として捉え，オフィス空間における場のセキュリティを考慮したリスクアセスメントとして，情報セキュリティの観点に物理セキュリティの観点を加えたリスク分析を行い，27 項目のリスク要因を抽出した．次に，これらのリスク要因に対し，リスクマトリクス手法に基づき，具体的なリスク対策案を提案し，情報セキュリティに物理セキュリティを加味した総合的なセキュリティ対策について示した．この結果，オフィス空間の場のセキュリティとして，具体的なリスク要因ならびに初歩的な対策案を明らかにした．

今後，さらに，法制度面も加味したより総合的なセキュリティ対策が可能となるように，検討を進めていくとともに，費用対効果も含めた具体的な対策案について検討していく．

謝辞

本研究は，JSPS 科研費 24300029 の助成を受けたものです．

参考文献

[1] 警察庁，平成 25 年中のサイバー犯罪の検挙状況等について，
http://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf
[2] 瀬戸洋一他，情報セキュリティの実装保証とマネジメント，日本工業出版，2009 年
[3] 情報セキュリティマネジメントシステム，JISQ27001，日本工業規格調査会
[4] JIPDEC，プライバシーマーク付与認定事業者数が 8,000 を超える，2011 年，
http://www.p-mark.info/list/index.html
[5] JIPDEC，認証取得組織数推移、認証機関別・県別認証取得組織数，2011 年，
http://www.isms.jipdec.jp/lst/ind/suii.html
[6] 米田翔一他，動的リスク評価に基づくセキュリティ場の提案，プロジェクトマネジメント学会 2013 年度春季研究発表大会，1501，pp303-307，2013
[7] 榎本真也他，ダイナミックに制御する情報漏洩対策システムの検討，FIT2012，L-034, 2012
[8] 末次正人他，侵入者の距離によりダイナミックにセキュリティレベルを制御するシステムの検討, 情報処理学会研究報告. 2013-CSEC-60(25), 1-6, 2013-03-07
[9] 谷本茂明他，個人のコンテキスト情報に基づく動的多重帰属グループサービスの提案，情報処理学会論文誌, Vol.51, No.2，575-589，2010
[10] JNSA，2011 年情報セキュリティインシデントに関する調査報告書〜個人情報漏えい編〜，
http://www.jnsa.org/result/incident/2011.html
[11] PMI：プロジェクトマネジメント知識体系ガイド第 4 版，2008
[12] NTT 情報流通プラットフォーム研究所，NTT R&D 情報セキュリティシリーズ，事例で学ぶ情報セキュリティマネジメント手法，2006 年