Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

情報持出時のセキュリティ対策についての一考察

新原功一† 内田勝也†

情報持出に係る情報漏洩事故の発生要因は，過失が大半を占めている．企業活動を営む上で，社外等に機密情報を持出す必要があるが，情報管理の責任は当事者に委ねられている．
本研究では，情報持出時のセキュリティ対策について，現状把握及び他分野でのヒューマンエラー対策事例等の調査を行った．その上で，当該組織の業務内容等を考慮して適切な対策を導き出すモデルを提案する．

Consideration on security measures at taking-out of confidential documents

Koichi Niihara† and Katsuya Uchida†

Fault consists mostly of occurrence factors of information leakage caused by taking-out of confidential documents. On business activities, it is sometimes necessary to take out confidential documents to the outside. However, responsibility of information management is left to the party in charge.
As for security measures at taking-out of confidential documents, this study conducted a survey on cases of understanding of actual state and countermeasures against human errors in other field. Then, we propose a model to lead appropriate measures in consideration of business of organizations concerned.

1. はじめに

情報持出に係る情報漏洩事故では，発生要因の大半が本人の意図に反する，即ち過失に起因している．企業活動を営む上で，社外等に機密情報を持出す必要があるが，情報管理の責任は持出し当事者に委ねられている．
本研究では，情報持出時において講じるべきセキュリティ対策について，現状把握及び他分野でのヒューマンエラー対策の調査を行った．それらから，当該組織の業務内容等を考慮して適切なセキュリティ対策を導き出すモデルを提案する．

2. 情報持出

2.1 情報持出とは

機密情報を取り扱うオフィスでは，大抵出入口の施錠管理がされており，エレベーターホールに警備員が常時監視されていることが多い．その他にも，真に重要な情報を取り扱う部屋では，生体認証による入退室管理や監視カメラなどによって，物理的セキュリティが確保されたスペースを設ける企業も多くなってきた．
また，自宅等はオフィスには及ばないものの，出入口の施錠管理等がされている．
一方で，外出先では物理的なセキュリティ対策を講じることは出来ない．そのため，比較的情報セキュリティの脆弱性，特に紛失や盗難に対するリスクが高くなると思われる．これらの関係を図 1 に示す．

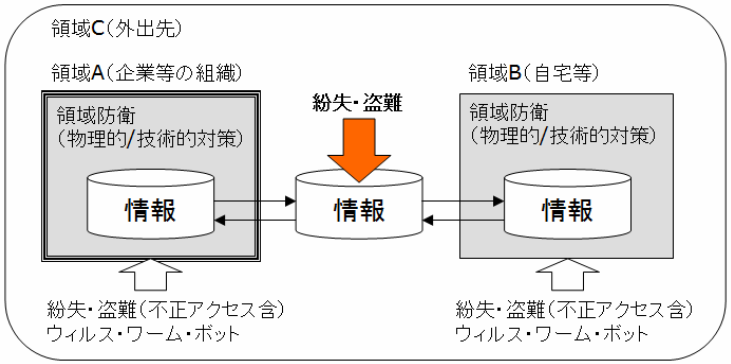

図 1 脆弱性が高い外出先*

図 1 のように外出先では盗難・紛失に対するリスクが高いことが想像できる．

† 情報セキュリティ大学院大学
Institute of Information Security
* 濱田 良隆,「情報持ち出し要因に関する共分散構造分析（仮題）中間発表会資料」の図を元に作成

Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

2.2 情報持出時の事故発生比率

自組織で発生したことがある情報漏洩事故について，情セ大 内田研究室による情報セキュリティ調査[1]† では，約 25%の組織が「ノート PC などの盗難」を挙げている．また，NRI セキュアテクノロジーズ社による調査[2]‡ では，約 27%の企業が過去 1 年間に発生した情報セキュリティに関する事件・事故として「携帯 PC 等の情報機器の紛失・盗難」をあげている．

上記のアンケートより，情報漏洩事故のうちパソコンの紛失･盗難を起因としたものが，一定の割合を占めていることがいえる．

2.3 情報持出時の事故の主な要因

次に，2007 年に公表された情報漏洩事故のうち，漏洩経路が「PC 本体」であったものの割合について，これらの事故に至った経緯を調べた．なお，項目の定義は，JNSA における調査報告書[3]に記されたものを利用した．

総数 94 件のうち，盗難が半分以上を占めていることが分かった．詳細を図 1 に記す．

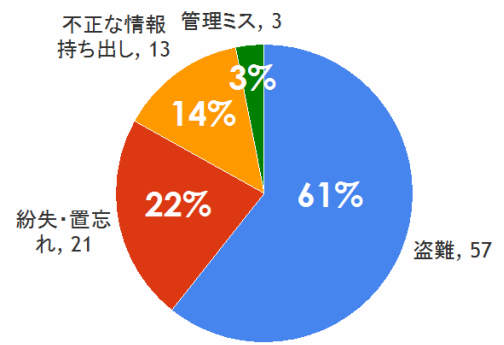

図 2 パソコンによる情報漏洩事故の内訳

「盗難」,「紛失・置忘れ」の 2 項目で全体の 83%を占めている．当事者の意図と反し、多くの事故が発生している．

2.4 情報持出の必要性

情セ大 内田研究室が，ISMS 認証取得組織に対して実施したアンケート調査[4]では，「パソコンを社外持出する際のルール」について質問している．

ISMS 認証取得業者は、ISMS 認証取得までの過程において情報セキュリティに対するルール整備が求められるケースが多いことから、「ルールなし」と回答した企業は無い．「社外持出全面禁止」は 7.3%、「ルールあり（持出許可必要）」は 87.5%である．

このアンケート結果から、大半の企業は業務の都合上，事業所外においてパソコンを利用する必要性があると考えているといえよう．

2.5 対策の実施状況

情セ大 内田研究室が，ISMS 認証取得組織に対して実施したアンケート調査[4]では，「業務用 PC の情報漏洩対策」について質問している．

この調査によれば，「ログインパスワード認証」,「ログインパスワードの定期的な変更」については，大多数の企業が実施している．また，「外部媒体の接続制限」は約半数の企業が実施しているが，「外部媒体のデータ移動時強制暗号」は 16%にとどまっている．このことから，外部媒体のリスクは認識しているもののコストが必要となる対策はあまり進んでいないことがわかる．

盗難・紛失等のリスクに対する対策としては，「保存ファイルの暗号化」,「BIOS パスワード設定」,「ハードディスク暗号化」は約 3 割の企業が対策している．

3. 他分野のヒューマンエラー対策

3.1 主な分析手法

航空，医療，電力，原子力，宇宙等様々な業界において，ヒューマンエラーの低減を目的として分析手法の開発が進められている．以下に，代表的な分析手法を列挙する．

- IRAS（Incident Report Analyzing System）[5]
- 4M-4E モデル
- SHEL モデル，P-mSHELL モデル
- バリエーションツリー分析手法（VTA），FTA（fault tree analysis），RCA
- H2-SAFER，Medical SAFER
- 4STEP/M
- J-HPES，人間エラー発生 FT 図法
- CREAM
- TapRoot

3.2 本研究で用いる分析手法

3.2.1 戦略的エラー対策の 4M

河野[6]によれば，エラー対策を戦略的に考えたときに，大きく 2 つに分けられる．1 つは「発生防止」であり，もう 1 つは「拡大防止」である．「発生防止」の段階では，できるだけヒューマンエラーの絶対数を少なくすることを考える．

STEP Ⅰ：危険を伴う作業遭遇数を減らす(Minimum encounter：機会最小)
STEP Ⅱ：各作業においてエラー確率を低減する(Minimum probability：最小確率)

† 企業・教育機関・自治体等を対象として 2007 年 1 月に実施
‡ 東証 1 部・2 部上場企業と従業員 300 人以上の非上場企業を対象として 2007 年 10 月に実施

Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

次に，拡大防止の段階では，ヒューマンエラーの発生はある程度避けられないという前提で考え，エラーが発生しても最終的には事故やトラブルに結びつかないようにする．

STEPⅢ：多重のエラー検出策を設ける(Multiple detection：多重検出)

STEPⅣ：被害を最小とするために備える(Minimum damage：被害局限)

各段階が，それぞれ M で始まることからこのエラー対策の考え方を「戦略的エラー対策の４M 」という．

3.2.2 エラー対策の思考手順

この戦略的エラー対策の 4M は，エラー対策を大まかに理解するためには有効だが，具体性が乏しい．そのため，河野は実行レベルまで分解した「エラー対策の思考手順」を提案している．

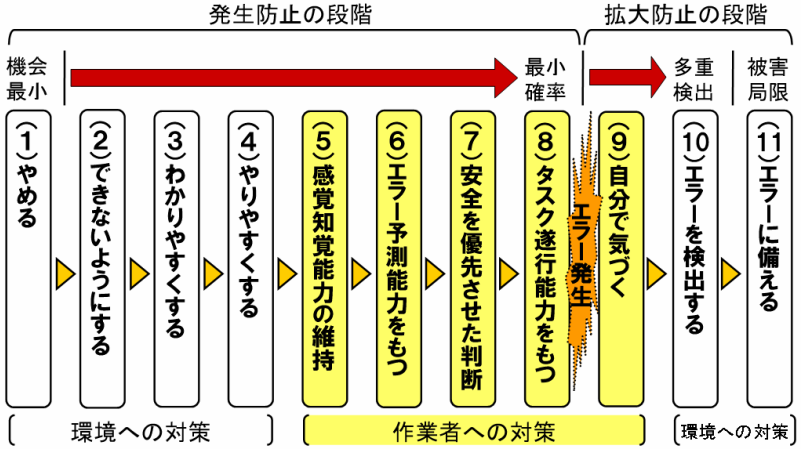

図 3 エラー対策の思考手順

このように思考手順にしたがって考えることによって，単なる思いつきの対策ではなく，対策を考えやすくなることが期待できる．なお，この思考手順では一般に左にいくほど大きな効果が期待でき，また人間への対策よりも環境への対策の方が効果を期待できるという特徴がある．

3.2.3 mSHEL モデル

航空分野には，当事者である人間が最適な状態を保つためには，４つの要因が影響しているということを表した SHEL モデルがある．

河野は SHEL モデルの改良を行い，m(マネジメント)を追加した m-SHEL モデルを提案している．更に医療分野向けに P（patient：患者）と L（Liveware：人）を追加した Pm-SHELL モデルを考案している．

3.2.4 発想手順マトリクス

河野[6]はエラー対策の思考手順と先述の P-mSHELL モデルを組み合わせ，エラー防止策の発想手順マトリクスを考案している．

4. 情報持出時に講じるべきセキュリティ対策

本章では，パソコンの情報持出時に講じるべきセキュリティ対策について，調査結果を述べる．また，それらの結果を整理して，課題や問題点の考察を行う．

4.1 対象範囲

まず，本論文において対象とする範囲を明確にする．

情報持出時とは，大きく分けて以下のような流れで行われることが多い．

フェーズ	内容
利用前	パソコンの準備，上長への持出許可
利用中	自組織－目的地間の移動，構外での作業
利用後	自組織にパソコンを持ち帰る．
盗難・紛失	パソコンを盗難・紛失する

表 1 情報持出に関する利用フェーズ

この表 1 で示されている項目のうち，「盗難・紛失」に対するセキュリティ対策を対象とする．なぜなら，「利用前」，「利用中」では

- 上長の承認を得ずに，パソコンを構外に持ち出した．
- カフェで，第三者に機密情報を盗み見された．

等といったケースは「問題」ではあるが，「盗難・紛失」した場合と比べて，リスクは軽微であるといえよう．また，「利用後」は組織内の物理的セキュリティに守られるため，こちらのリスクはもっと低くなる．

その点，特に問題となるのがパソコンを「盗難・紛失」をした場合である．企業等では，このような事故が発生した場合，たとえ当該機器に相当レベルのセキュリティ対策が講じられていたとしても，その事実を公表している．

次節以降、セキュリティ対策の洗い出しを行うが、「利用前」，「利用中」「利用後」のフェーズは，比較的リスクが低いことから，「盗難・紛失」に対するセキュリティ対策を対象とする。

4.2 セキュリティ対策の洗い出し

4.2.1 既存ドキュメントの調査

関連する規格やガイドラインなどの既存ドキュメントについての調査を行い，記述内容の整理を行った．調査対象のドキュメントは，国内における組織が利用しやすいものを選んだ．情報持出時のセキュリティ対策について，記載されていたのは以下のドキュメントである．

・ JISQ 27002:2006 (情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範)
・ PCI DSS バージョン 1.2(要件とセキュリティ評価手順)

なお，上記以外には COBIT4.1，NIST SP800-30 も調査をしたが，情報持出時におけるセキュリティ対策の記述は見当たらなかった．

4.2.1.1. JIS Q 27002

JIS Q 27002 では，主に以下のような対策が記載されていた．

項番	内容
9.2.5§	無人の状態で放置禁止，情報持出時の管理者による事前許可，
11.7.1**	盗難，置き忘れからの物理的な保護，暗号技術による保護，ネットワーク接続における保護，保護されていない場所での作業リスクの考慮，インシデント対応手順策定，無人の状態で放置禁止，モバイル設備を用いる要員の意識向上のための教育・訓練を計画

表 2　JIS Q 27002 に記載された情報持出時の主な管理策††

様々な管理策を挙げられていることが分かる．一見すると，これらの対策を実施していれば，リスクはかなり低減されるようにみえる．

しかしながら，これらの管理策は，箇条書きで羅列されており，物理的対策，技術的対策，人的対策の区分けや，どの時点で講じるべき対策なのか（モバイルコンピュータの持出前，持出中，紛失に備える対策）等の記述はない．そのため，記載内容から類推する必要が生じる．従って，このままではセキュリティ対策が必要かつ十分なものであるか，判断をすることはできない．詳しくは後述するが，JIS Q 27002 の管理策は技術的な対策に偏っており，「紛失・盗難」に対する管理策は殆どが被害拡大を防ぐものであり、「紛失・盗難」の発生を防ぐものではなかった．

4.2.1.2. PCI DSS

PCI DSS では，主に以下のような対策が記載されていた．

項番	内容
8.3‡‡	２因子認証の導入（ダイアルアップ認証とトークン，又は VPN と個々の証明書など）
12.3.10§§	遠隔アクセス時の情報保存禁止

表 3　PCI DSS に記載された情報持出時の主な管理策***

§ 9.2.5 構外にある装置のセキュリティ
** 11.7.1 モバイルのコンピューティング及び通信
†† 管理策を筆者にて意訳
‡‡ 要件 8: コンピュータにアクセスできる各ユーザに一意の ID を割り当てる。
§§ 要件 12: 従業員および派遣社員向けの情報セキュリティポリシーを整備する。
*** 管理策を筆者にて意訳

PCI DSS は，技術的な対策に偏っているが，JIS Q 27002 と比較すると，具体的な対策内容の明記がされていた．また，両ドキュメントの記載内容に重複はなかった．

4.2.2 ヒューマンエラー対策

情報持出による事故の原因は，大半が過失であることから，ヒューマンエラー対策のうち，情報持出時にて講じるべきセキュリティ対策の抽出を行った．

抽出にあたっては，主に河野による医療分野におけるヒューマンエラー対策の事例を参考とした．抽出した対策は，エラー対策の思考手順(3.2.2 参照)に分類した．結果を表４に記載する．

エラー対策の思考手順	内容
①やめる（なくす）	外出時に必要な情報以外保存しない．
②できないようにする	ー
③わかりやすくする	パソコンに注意喚起のシールを貼る
④やりやすくする	軽量なパソコンの利用,持出専用のバッグに荷物をまとめ，手荷物を２つ以上持たない
⑤知覚能力を持たせる	適切な休息をとる，飲酒をしない
⑥認知・予測させる	ヒヤリ・ハット事例の共有化，KYT（危険予知トレーニング），ヒューマンエラー工学の知識の習得
⑦安全を優先させる	明確な判断基準の整理（網棚にパソコンを置かない，車内ではトランクに保管など）
⑧できる能力を持たせる	ポリシーや判断基準の理解度をテストし,合格者のみ持出を許可,応用行動分析によるインシデント発生防止教育
⑨自分で気づかせる	指差呼称
⑩検出する	同行者によるダブルチェック
⑪備える	ー

表 4　情報持出時におけるヒューマンエラー対策

JIS Q 27002,PCI DSS では，記載が少なかった「人的対策」を補完することができた．

4.2.3 その他の技術的な対策

その他の技術的対策として，セキュリティ関連企業が公開している製品情報を収集し、シンクライアントやパソコン遠隔監視システム，生体認証によるログイン制限等を対策として追加した．

4.3 網羅性の検証

4.3.1 エラー対策の発想手順マトリクスへのマッピング

4.2 にて洗い出した調査したセキュリティ対策について，漏れ抜けが無いかを確認するため，エラー対策の発想手順マトリクス(3.2.4 参照)にマッピングして網羅性の検

Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

証を行った．なお，エラー対策の発想手順マトリクスを構成している PmSHELL モデルのうち、P(患者)は今回のケースでは存在しない．また「当事者＝被害者」であるため，L も一人である．そのため、P と L を除いたｍSHEL モデルに修正した．この修正した発想手順マトリクスにセキュリティ対策をあてはめた．結果を図 4 に記載する．

4.3.2 結果の分析

前節の結果について、特徴的なものを以下に記す．

・JIS Q 27002 PCI DSS の管理策は，殆どが「①やめる（なくす）」か「⑪備える」に該当

盗難・紛失にあった場合、たとえ当該機器の機密情報の暗号化やログインパスワードを複雑化等の対策を講じていた場合でも、高度な技術をもった人間であれば中身を解析することは可能であり、情報漏えいのリスクが残ることから，その事実を世間に公表しなければならないことがある．この場合，企業イメージも損なわれ，インシデント対策費用は膨大なものとなることが想定される．

一方で，仮に JIS Q 27002， PCI DSS の管理策は，殆どが「⑪備える」に対する対策となっていた．この「⑪備える」は，あくまで被害を最小限に食い止めるものであって，「紛失・盗難」の発生自体を防ぐものではない．

「⑪備える」の対策ばかりを講じて、情報持出に対するセキュリティ対策をやったつもりになっていても、実は「盗難・紛失」の発生のリスクに対してほとんど無防備となっているといえる．もっといえば，「盗難・紛失」が発生しないのは当事者がたまたまミスを犯さないだけ，なのである．そして，人間はミスを犯す動物であることから，ミスが発生して，それが事故発生に直結してしまうのである．

・その他の技術的対策である「シンクライアント」「遠隔データ消去，位置情報特定」といったサービスも「⑪備える」に該当

「シンクライアント」，「遠隔データ消去，位置情報提供サービス」も「盗難・紛失」の発生自体を防ぐことはできない．「位置情報提供サービス」は，一見すると「盗難・紛失」にあったパソコンを見つけられるので，発生を防ぐことができるように見えるが，現在の GPS の精度は条件が良い場合でも数メートルとなっており，高層ビルが立ち並ぶオフィス街において盗難にあった場合，見つけるのは困難な場合もあることを認識しておく必要がある．

・E(環境)への対策を講じることが出来ない．

構外に情報を持出すということは，自組織のマネジメントを及ばない環境に情報を持出すことを意味する．環境を変えることができないため，情報管理の責任は持出当事者に委ねられることになる．

・ヒューマンエラー対策は，「③わかりやすくする」から「⑩検出する」まで様々な対策を講じることが可能

4M	対象		m(マネジメント) 風土、組織を変える	H(ハードウェア) 設備を変える	S(ソフトウェア) 手順、ソフトウェアを変える	E(環境) 環境を変える	L(当事者) 当事者が変わる
機会最少	環境への対策	①やめる（なくす）	[J]モバイルコンピュータの構外持出を禁止する		[P]遠隔アクセス時の情報保存禁止		
			[H]外出時に必要な情報以外保存しない。				
		②できないようにする					
		③わかりやすくする	[J]モバイルコンピューティング方針の策定	[H]パソコンに注意喚起のシールを貼る（紛失注意等）			
		④やりやすくする		[H]軽量なパソコンの利用 [H]持出専用のバッグに荷物をまとめ、手荷物を2つ以上持たない			
最小確率	作業者自身への対策	⑤知覚能力を持たせる					[H]適切な休息をとる [H]飲酒をしない [H]Ｉｍ safeの利用
		⑥認知・予測させる	[H]ヒヤリ・ハット事例の共有化				[H]ヒヤリ・ハット事例の共有化 [H]KYT（危険予知トレーニング） [H]ヒューマンエラー工学の知識の習得
		⑦安全を優先させる					[J]無人の状態で放置禁止（重要度高の情報が格納された場合） [J]モバイルPCのカモフラージュ（パソコンの存在を外部に分からないようにする）
			[H]明確な判断基準の整理（網棚にパソコンを置かない、車内ではトランクに保管等）				[H]明確な判断基準の整理（網棚にパソコンを置かない、車内ではトランクに保管等）
		⑧できる能力を持たせる	[J]モバイルコンピューティング取扱研修の計画				
							[H]持出前に、ポリシーや判断基準の理解度をテストし、合格者のみ持出を許可 [H]応用行動分析によるインシデント発生防止教育
		⑨自分で気づかせる					[H]指差呼称
多重検出	環境への対策	⑩検出する		[他]利用者と対象物が数m以上離れると警告する機器をパソコン、鞄等に装着			[H]同行者によるダブルチェック
被害局限		⑪備える	[J]盗難、紛失時のインシデント対応手順策定	[J]ジェラルミンケース等に施錠保管 [P]2因子認証の導入	[J]暗号技術によるデータ保護 [J]アクセス可能領域の制限 [P]2因子認証の導入		
				[他]利用者以外の生体認証によるログインを制限 [他]遠隔データ消去、GPSによる位置特定 [他]シンクライアントの導入	[他]遠隔データ消去、GPSによる位置特定 [他]遠隔データ削除ツールを利用		

【凡例】[J]JIS Q 27002，[P]PCI DSSv1.2，[H]他分野のヒューマンエラー対策，[他]その他の技術的対策

図 4 エラー対策の発想手順マトリクスによる整理結果

Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

4.2.2 で抽出したヒューマンエラー対策では，様々なフェーズの対策が存在する．「①やめる」から「⑧出来る能力を持たせる」のフェーズの対策を講じることによって、特に事故の発生を未然に防止することが期待できる．

4.4 考察

エラー対策の発想手順マトリクスにセキュリティ対策をマッピングすることで，様々な角度から情報持出時のセキュリティ対策として考えられるものを洗い出すことができた．特に，ヒューマンエラー対策を参考とすることで，各作業においてエラー確率を低減する「最小確率」のフェーズにおける対策を多く抽出することができた．

しかし，これらの対策を講じるためには，時間，コスト，労力，ノウハウ等が必要である．企業活動は，リスク低減だけに経営資源を費やすわけにはいかない．

一方，情報持出の必要性について考えてみると，オフィス内で事務処理を中心とした業務を担う部門と，顧客への営業活動で社員が各地を飛び回っている部門では，持出をする期間，頻度，内容などは大きく異なる．この両者では，当然「盗難・紛失」のリスクには大きな差があるだろう．

当然のことだが、リスクが異なるのであれば講じるべき対策も異なってくる。そこで，次章では業務内容等を考慮して適切なセキュリティ対策を導きだすためのモデルを構築する．

5. 情報持出時のセキュリティ対策モデル

本章では，業務内容等を考慮した適切なセキュリティ対策を講じるためのモデルを提案する．そして，4 章で抽出したセキュリティ対策を当該モデルに適用する．最後に考察を行う．

5.1 業務フローの洗い出し

まず，適切なセキュリティ対策を導き出すために，まず当該組織の業務のうち，情報持出に係る業務の業務フローの作成をおこなう．その際，フロー自体に無駄な工程がないかを確認することが必要である．

5.2 業務パターンによる分類

構外に持ち出す期間によって，盗難・紛失のリスクは変化する．当然，短い期間しか持ち出さなければ，ヒューマンエラーが発生する確率も下がる．逆に，常時パソコン等を構外に持ち出している場合，ヒューマンエラーが発生する確率は高くなり，盗難・紛失にあう頻度も多くなる．

そこで，適切なセキュリティ対策を講じるため業務パターンとして，3 つのパターンを作成した．表 5 に業務パターンを記す．

業務パターン	説明	紛失･盗難のリスク
パターン① 日勤帯	出社して，退社するまでにパソコンの持出，構外での業務，パソコンの持ち帰りまでが可能	比較的低い
パターン② 短期出張	地方出張や短期の海外出張など，短期間（1 週間未満）の宿泊が伴い，現地にて機密情報の取り扱いをする必要があるもの	中程度
パターン③ 長期出張 常時持出	長期出張（1 週間以上）や外回りの営業マンなど日常的な業務が構外中心となっているもの また，常時持出の許可を与えているもの	高い

表 5　情報持出時における業務パターン

5.3 セキュリティ対策の分類

情報持出時にセキュリティ対策は，5 つに分類した．モデルⅠ，Ⅰ’は共通対策として，どの業務パターンでも講じるべきもの，モデルⅡ，Ⅲ，Ⅳはパターン毎に応じて，講じるべきものとした．当該モデルの定義を表 6 に記す．

モデル	定義	対象パターン
モデルⅠ 共通	情報持出をする際には，最低限実施すべき対策	①/②/③
モデルⅠ’ 共通（任意）	情報持出をする際には，実施することが望ましいが，対策費用が高額であるため，必要に応じて実施することが望ましい対策	①/②/③
モデルⅡ 短期持出	情報持出をする際には，実施することが望ましいが，長期出張時には業務に支障があり，実施することが困難な対策	①/②
モデルⅢ 宿泊	宿泊に伴うリスクに対して，実施すべき対策	②/③
モデルⅣ 長期持出	情報持出しの機会が多く，紛失・盗難のリスクが高いことから，より一層のリスク低減が必要な場合に実施すべき対策	③

表 6　情報持出時のセキュリティ対策のモデルの定義

次に、業務パターンとモデルの関係について、図 5 に記す．

例えば、業務パターン②の場合、モデルⅠ、Ⅰ’、Ⅱ、Ⅲに該当する対策を講ずることになる。このようにして、各対策を複合的に組み合わせることで「盗難・紛失」

Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

のリスク低減を図る。そして、4 章で整理したセキュリティ対策に対して，当該モデルを適用した結果を図 6 に記す．このモデルによって，業務内容毎に講じるべきセキュリティ対策を確認することが可能となる．

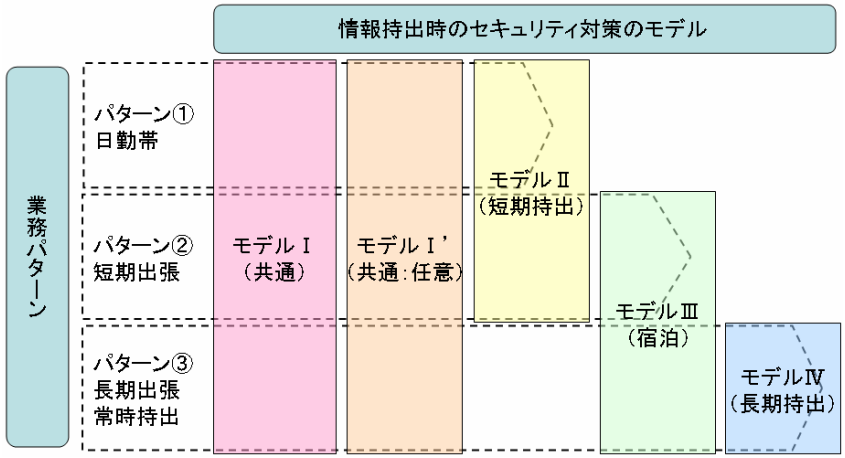

図 5 業務パターンとモデルの関係

5.4 評価と考察

業務パターン毎に講じるべきセキュリティ対策を分類することにより，業務内容に応じたセキュリティ対策を構築するためのモデルを作成することができた．

また，4 章にて，情報持出時に構ずるべきセキュリティ対策を洗い出したものを当該モデルに適用することによって,適切なセキュリティ対策を導き出すことができた．ただし，いくつかの課題もみつかった．

(1) 長期出張等の発生頻度が極端に少ない（年に 1 回程度）場合の課題。

モデルⅣを適用する基本的な考え方としては，あくまで長期出張や構外での営業活動が定常業務となっているかどうかを見極める必要がある．例えば，モデルⅣの対策の一つにヒヤリ・ハット事例の共有化があるが，そもそも発生頻度が少ない場合にはヒヤリ・ハット事例自体が発生しない．応用行動分析によるインシデント発生防止教育についても，インシデント自体が発生しないことには発生の防止ができない．

唯一，KYT（危険予知トレーニング）であれば，想定事象を用意したトレーニングをすることは可能であるが，このような教育プログラムを作成する事自体も費用がかかる．費用対効果を考えた場合，果たして実施すべきかどうかについては，持出す機密情報の重要度等を考慮して判断をする必要がある．

4M	対象		モデルⅠ 共通	モデルⅡ 短期持出	モデルⅢ 宿泊	モデルⅣ 長期持出
機会最少	環境への対策	①やめる（なくす）		外出時の持出情報を最低限にする。 遠隔アクセス時の機密情報保存禁止		
最小確率	環境への対策	②できないようにする	アクセス可能領域の制限 2因子認証の導入			
		③わかりやすくする	パソコンに注意喚起のシールを貼る（紛失注意等） モバイルコンピューティング方針の策定			
		④やりやすくする	軽量なパソコン利用 持出専用バッグ用意 手荷物を2つ以上持たない			
	作業者自身への対策	⑤知覚能力を持たせる	I'm safeの利用		適切な休息をとる 飲酒をしない	
		⑥認知・予測させる			ヒューマンエラー工学の知識の習得（記憶力の限界等）	ヒヤリ・ハット事例の共有化 KYT（危険予知トレーニング）
		⑦安全を優先させる	無人状態放置禁止 モバイルPCのカモフラージュ 明確な判断基準の整理 （網棚にパソコンを置かない、車内ではトランクに保管等） モバイルPC取扱研修計画			
		⑧できる能力を持たせる			持出許可前に、ポリシーや判断基準の理解度をテストし、合格者のみ許可	応用行動分析によるインシデント発生防止教育
		⑨自分で気づかせる	指差呼称			
多重検出	環境への対策	⑩検出する		利用者と対象物が数m以上離れるとアラームが鳴る機器をパソコン、鞄等に装着 同行者によるダブルチェック		
被害局限	環境への対策	⑪備える	ジェラルミンケース等に施錠保管 暗号技術によるデータ保護 盗難、紛失時のインシデント対応手順策定 ※以下モデルⅠ’ ログイン時生体認証 遠隔データ消去、GPS位置特定			モバイルシンクライアント導入

図 6 エラー対策の発想手順マトリクスによる整理結果

Vol.2010-DPS-142 No.46
Vol.2010-CSEC-48 No.46
2010/3/5

(2) モデルⅠの対策を実施する経営資源が不足している場合の課題

組織によっては，従来業務に経営資源の殆どが費やされ，セキュリティ対策に対する人員，費用等が不足している場合がある．

当然のことだが，リスク低減の施策を行わなければ，リスク自体を低減することは出来ない．一方で，経営資源が不足している場合でも，費用が殆どかからない対策（パソコンに注意喚起のシールを貼る，I'm Safe の利用，明確な判断基準の整理，指差呼称等）は実施することは可能だろう．リスク低減を低減するための努力は怠らないことが，情報漏えい事故の発生防止につながるのではないかと考える．

(3) 業務パターン①の場合，モデルⅢ，Ⅳの対策が軽視される可能性がある

業務パターン①の場合，当該モデルではモデルⅠ，Ⅰ'，Ⅱを講ずるべきとしている．一方で，モデルⅢ，Ⅳの対策は対象外となっている．対象外となっているから，実施する必要がない訳ではなく，仮に機密性の高い情報を持出すことが多い場合などには，これらの対策を組織内で実施することは，リスク低減に貢献することができる．

6. おわりに

本研究では，業務内容等を考慮して適切なセキュリティ対策を導き出すモデルを構築し、考察を行った．情報持出時のセキュリティ対策では，構外での作業となるため人的対策に依存するところが大きい．そこでは，ヒューマンエラーの発生自体は前提として，継続的に多重のセキュリティ対策を講じていくことが重要である．当該モデルを活用することで，情報持出時の情報漏洩事故の発生が抑制されることを期待している．

参考文献

[1] 情報セキュリティ大学院大学内田研究室、「第 5 回情報セキュリティ調査から見た情報セキュリティ状況の比較」、2008
[2] NRI セキュアテクノロジーズ、「企業における情報セキュリティ実態調査 2007」、2007
[3] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ、「2007 年情報セキュリティインシデントに関する調査報告書 Ver. 1.6」、2009
[4] 情報セキュリティ大学院大学内田研究室、「ＩＳＭＳ（情報セキュリティマネジメントシステム）第三者認証制度及びその実態調査」、2009
[5] 宮城雅子、「大事故の予兆をさぐる―事故へ至る道筋を断つために」、講談社ブルーバックス、1998
[6] 河野龍太郎、「医療におけるヒューマンエラー―なぜ間違えるどう防ぐ」、医学書院、2004