EC における情報セキュリティに関する活動報告書 2009

（情報セキュリティ WG：SWG1・SWG2・TF の各報告書）

平成 22 年 3 月

次世代電子商取引推進協議会

はじめに

本報告書は、次世代電子商取引推進協議会において、2009 年度に実施した情報セキュリティワーキング（WG）活動の内、傘下の二つのサブワーキング（SWG1&2）及び一つのタスクフォース（TF1）の推進内容と成果をまとめて、全体として報告するものである。

報告書内容は下記の通り、各々独立した三部構成としてまとめているので、詳細については、各報告書を参照ください。

記

活動	各報告書名称
SWG1	「セキュリティ評価チャートモデル策定業務についての調査検討報告書 2009（SWG1）」
SWG2	「EC の情報セキュリティ推進に不可欠な項目調査研究活動報告書 2009（SWG2）」
TF1	「秘密分散技術利活用検討における活動成果報告書 2009（TF1）」

次世代電子商取引推進協議会
情報セキュリティ WG 事務局

セキュリティ評価チャートモデル策定業務についての調査検討報告書 2009（SWG1）

― 企業組織における機密情報管理の実態調査と

情報セキュリティガバナンスの支援策検討 ―

平成 22 年 3 月

次世代電子商取引推進協議会 情報セキュリティ WG

（SWG１）

はじめに

本報告は、保護を必要とする個人情報や企業情報（設計図等）など、重要な業務データ（以下では、機密情報と呼ぶ）やその取扱プロセスに対して、企業内での保管や組織間での受け渡しのリスクに関する責任分界点を表現する業務データプロセスセキュリティ評価チャート1を組織間で共通理解に利用することを普及させ、情報セキュリティガバナンスの向上を支援することを目的とする。

このセキュリティ評価チャートは、機密情報の発生から消滅するまでのライフサイクルに着目し、その情報の収集・保管・受け渡し・利用・廃棄に関して、いつ、だれが、どのように取り扱うかを人的作業と計算機処理に分けて明記する。これにより、機密情報にかかわる情報セキュリティの責任分界点と対策・作業の責任分担を明確化するものである。

既に、先進企業では委託業務の守秘義務契約等で、企業間や企業内の異なる組織の間での情報セキュリティ対策の共通理解の道具として利用されている。これにより、リスクが少なく作業効率のよい業務への改善、抜けのない効果的なセキュリティ対策の推進などに効果を上げている。

本報告では、情報セキュリティガバナンスの向上の具体策としてセキュリティ評価チャートを普及させていくことを目的とし、企業における情報セキュリティ対策の実態調査とセキュリティ評価チャートの書き方を報告するものである。本アプローチにより企業間や企業内で責任分界点を明確化し、情報セキュリティガバナンスの向上を支援することに資すれば幸いである。

日本情報処理開発協会　電子商取引推進センター
（次世代電子商取引推進協議会 情報セキュリティ WG）

[1] 次世代電子商取引推進協議会（ECOM）にて共通化を検討した機密情報の管理フローを示すモデル

目 次

1. 活動概要 … 1
1.1. 経緯と目的
1.2. 活動の内容と経過

2. 企業における機密情報管理の実態調査 … 3
2.1. 調査方法 … 3
2.2. アンケート調査結果 … 4
2.2.1. 回答者の概要
2.2.2. 情報セキュリティ対策の実態ついて
2.2.3. セキュリティ評価チャートの適用可能性について
2.3. ヒアリング調査結果 …12
2.3.1. 回答者の概要
2.3.2. セキュリティ評価チャートの有効性について
2.3.3. 各企業での導入の可能性について
2.4. 実態調査のまとめ …23
2.4.1. これまでの情報セキュリティ対策の効果
2.4.2. セキュリティ評価チャート導入への課題

3. 情報セキュリティの見える化 …27
－業務データプロセスセキュリティ評価チャート作成マニュアル―
3.1. セキュリティ評価チャートの使い方 …27
3.1.1. 人情報保護ガイドラインの改訂
3.1.2. セキュリティ評価チャートの利用
3.1.3. チャートの効果
3.2. セキュリティ評価チャートの書き方 …29
3.2.1. 記載内容
3.2.2. 記述形式
3.2.3. 評価チャートのフォーマット
3.3. 使い方の例 …32
3.3.1. 事例 A：委員会設置から謝金支払・報告書配布
3.3.2. 商品説明会（イベント）参加者募集から参加者報告の業務委託
3.3.3. 入札時の技術審査フローの記述と業務の改善
3.4. 書き方のノウハウ …37

4. 今後の課題 …39
4.1. 普及活動 …39
4.2. 標準化活動（国内、海外） …40
4.3. 契約等の法律的な縛りの検討 …40
4.4. リスク評価、対策導出方法（技術開発） …41

参考文献・資料 …42

情報セキュリティ WG（SWG1）メンバーリスト …43

付録 …44
A. アンケート依頼 …44
B. アンケート集計 …46
C. ヒアリング内容 …51

1. 活動概要

1.1. 経緯と目的

日本では平成 17 年 3 月に個人情報保護法が全面施行され、各省庁では個人情報保護法ガイドライン[1]などを作成し、その普及啓発を進めた。各企業は個人情報を中心として情報セキュリティ対策を実施してきた[1]。日本のプライバシーマーク取得事業者[2]は 1 万社、情報セキュリティ管理システム（ISMS）の認定事業者[3]も 3 千社を超えた。情報セキュリティ対策を実施してきた企業では、会社幹部や従業員の意識向上、機密情報資産の整理、様々な取扱ルールの設定が実施され、企業内の情報管理能力が向上してきている。

日本の情報社会では、インターネットによる企業間の電子商取引が 160 兆円程度となり、企業消費者間の電子商取引も 6 兆円を超え、世界でも最大規模の電子商取引（EC）となった[4]。EC の拡大にともない、情報犯罪は愉快犯から経済犯へと変貌し、その手口は年々に巧妙化してきている[5]。犯罪の手口が巧妙化するほど、一企業が自助努力で対応することが厳しいものとなってきている。電子化された情報を利活用することが前提となった今日の情報社会で、情報セキュリティ対策の弱い企業で事件・事故が発生する。情報セキュリティ対策を施した企業でも、新たに発生する脅威への対応も必要であり、事件・事故の発生が収束していないのが実情である。

このような背景を鑑み、平成 17 年度より次世代電子商取引推進協議会（ECOM）では電子商取引における情報セキュリティに関する活動を行ってきた[6]。平成 20 年度には業務委託をテーマとし、異なる組織間での情報保護連携に向けて、「業務データプロセスセキュリティ評価チャート」による情報セキュリティの責任分界点と責任分担の明確化を進める活動を行ってきた[7]。本報告は、経済産業省 委託事業「情報セキュリティガバナンス向上の具体策」として企業での情報セキュリティ対策の実態を報告し、「業務データプロセスセキュリティ評価チャート」を提案するものである。

1.2. 活動の内容と経過

本年度は、情報セキュリティ対策推進のガバナンス向上の具体策として、セキュリティ評価チャートの普及と共通化を目指して、企業における機密情報管理の実態調査、セキュリティ評価チャートの書き方の整備を行った。

なお、11 月より、経済産業省「情報セキュリティ対策推進のガバナンス向上の具体策」の委託事業に参画し、以下の活動を推進した。活動内容と経過を表 1.1 に示す。

(1) 企業における機密情報管理の実態調査
・アンケートによる実態調査
・ヒアリングによる実態調査

(2) セキュリティ評価チャートの書き方の整備
・適用事例の作成
・書き方ガイドの作成

表 1.1. 活動経過

活動内容	(期日)
第 1 回 WG	(平成 21 年 6 月 26 日)
・平成 20 年度 企業間情報保護連携の活動成果について ・平成 21 年度 企業間情報保護連携(SWG1)活動の活動計画(案)の検討	
第 2 回 WG	(平成 21 年 9 月 8 日)
・セキュリティ評価チャートの適用シーンと事例の意見交換	
第 3 回 WG	(平成 21 年 11 月 13 日)
・セキュリティ評価チャートの書き方のマニュアル(案)について ・企業における機密情報管理の実態調査のアンケート実施内容の検討	
アンケート実施	(平成 21 年 12 月 18 日～平成 22 年 1 月 10 日)
・ECOM 会員及び個人情報等を取扱う各企業(依頼先:162 社・回答 20 社)	
第 4 回 WG	(平成 22 年 1 月 19 日)
・アンケート実施結果の報告 ・企業の情報管理の実態に関する意見交換	
ヒアリング実施	(平成 22 年 1 月 22 日～2 月 10 日)
・金融、製造、流通、物流、情報システムベンダ、他	
第 5 回 WG	(平成 22 年 3 月 20 日頃予定)
・ヒアリング実施結果の報告 ・今年度の活動成果報告書のレビュー	

2. 企業における機密情報管理の実態調査

情報セキュリティ対策推進のガバナンス向上の具体策の検討として、「企業における機密情報の取り扱いとリスクの把握」について、アンケート調査とヒアリング調査を行った。アンケートでは本アプローチのニーズを調査し、ヒアリングでは本アプローチの普及課題を中心に調査を実施した。アンケートは「情報セキュリティ対策の実態」と「セキュリティ評価チャートの適用可能性」の設問項目からなり、次世代電子商取引推進協議会(ECOM)会員企業を中心にアンケートを実施した。ヒアリングは本アプローチに関心のある回答者に対しては、個別に調査を行った。また、委員会(WG)を開催し、アンケート回答をもとに企業の情報管理の実態とセキュリティ評価チャートの適用可能性について、情報セキュリティ WG メンバーと忌憚のない意見交換を行った。本章では、調査の目的と方法、アンケートとヒアリングの調査結果および、WG メンバーでの意見交換の結果を示す。

2.1. 調査方法

個人情報保護法の施行(平成 17 年度以降)に行ってきた各企業の情報セキュリティ対策が業務に与えた影響、幹部と従業員の認識の変化、セキュリティ評価チャートの適用可能性（ニーズ）と各企業での導入の可能性を調査の目的とした。アンケート調査とヒアリング調査の方法は以下のとおりである。

(1) アンケート調査

アンケートの設問項目は情報セキュリティ対策の実態に関する項目とセキュリティ評価チャートの適用可能性に関する項目とした。情報セキュリティ対策の実態については、平成 19 年 3 月の「ISMS の維持管理における実態調査」報告書[8]を参照し、業務に与えた影響、幹部と従業員の認識に関する設問とした。また、セキュリティ評価チャートの適用可能性については、機密情報の取り扱いでヒヤリ、ハットした情報管理の実態とその改善に向けた具体的な取り組みに関する設問を用意した。アンケートの期間、依頼先、設問項目の概要は下記のとおりである。なお、詳細な設問内容については付録 A を参照されたい。

■期　　間：H21.12.18.～H22.1.7.（3 週間）
■依 頼 先：ECOM 会員及び個人情報等を取扱う各企業（150 社）
■設問項目の概要：
－情報セキュリティ対策の実態について
・2005 年以降の対策の効果と業務に及ぼした影響
・情報セキュリティ対策への組織幹部と従業員の認識
・今後の対策として必要と思う分野と基盤
－セキュリティ評価チャートの適用可能性
・ヒヤリ、ハットした情報管理の存在、責任分界点の明確化
・機密情報の責任分担の明確化
・セキュリティ評価チャートの利用と標準化

(2) ヒアリング調査

アンケート調査に対し、ヒアリングではセキュリティ評価チャートの適用可能性を中心の設問項目を設定し調査を行った。設定したヒアリング項目は業務別の適用の可能性と各企業におけるセキュリティ評価チャートの導入の可能性を調査した。ヒアリング先は、問題意識の高いアンケートの回答者とし､あらかじめメールでヒアリング項目[付録 C]を提示した上で、対面およびメールによる聞き取りを行った。

■期　　間：2 週間（H22.2.3.～H22.2.10.）
■依 頼 先：金融、製造、情報サービス、システムソフトベンダ、他
■設問項目の概要：
－セキュリティ評価チャートの適用可能性
・機密情報管理（受け渡しや格納）での有効性
・企業内や企業グループ内の内部統制での有効性
・委託業務・アウトソーシングでの有効性
・国際取引での有効性での有効性
－セキュリティ評価チャートの導入可能性
・各企業における導入の可能性
・各企業における導入の課題

2.2. アンケート調査結果

2.2.1. 回答者の概要

アンケート回答数は 19 件(回答率：12.6%)であった。主な回答者の業種・業態は情報システムベンダ、担当職種はセキュリティ企画部門であった。その内訳を以下に示す。

(1) 業種･業態別の回答数(回答数 19 件)

①金融：2 件、②製造：3 件、③流通：1 件、④電力：2 件、⑦賃貸業：1 件、
⑤情報サービス提供業：1 件、⑥情報システムベンダ：8 件、
⑧非営利団体：1 件

(2) 担当職種別の回答数(回答数 21 件、重複含む)

①管理担当取締役：1 件、②内部統制担当：1 件、③ECOM 会員窓口：5 件
④セキュリティ企画部門：9 件、⑤部門セキュリティ担当：2 件、
⑥情報システム部門：1 件、⑦SE：1 件、⑧一般社員：1 件

2.2.2. 情報セキュリティ対策の実態ついて回答

今回のアンケート実施規模が小さく、定量的な評価としては回答数が少ない。以下では、定性的な結果として半数以上もしくは、4 分の 1(数名)の回答が得られた内容を中心に調査結果を示す。本章では、平成 19 年 3 月に ISMS の維持管理の実態について実態報告（回答 162 社）の調査結果[8]を踏まえ、今回の調査結果を報告する。なお、アンケートの集計データは付録 B を参照されたい。

(1) 2005 年以降の対策の効果と業務に及ぼした影響

対策成果として、半数以上が「情報流出や漏えいの防止・軽減」、「情報資産の明確化と整理」、「社員意識の浸透と実践」、「事故発生時の体制の整備」と回答したにもかかわらず、「セキュリティ事件・事故の減少」という回答は 4 分の 1 程度であった[設問 1-1]。

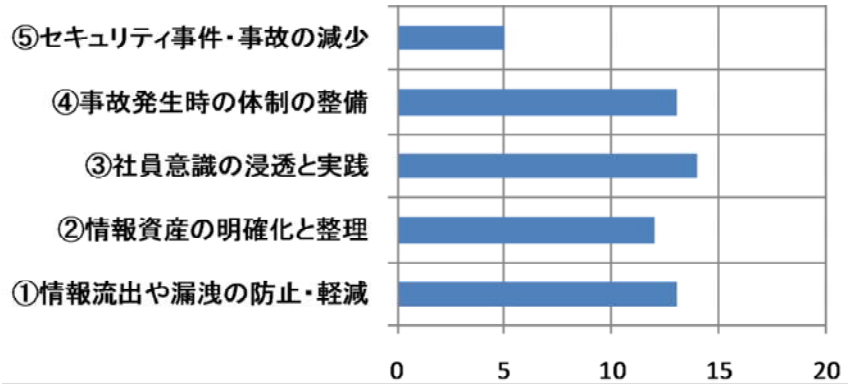


図 2.1-1 2005 年以降の情報セキュリティ対策で得られた効果は？

業務に及ぼした影響としては、半数以上が「対策コストの増加」「業務上の制約の増加」と回答し、「手続きの煩雑化・業務効率の低下」「業務上の制約の増加」、についても半数近い回答であった。それに対して「対策要員の増加」という回答は 4 分の 1 以下であった[設問 1-2]。

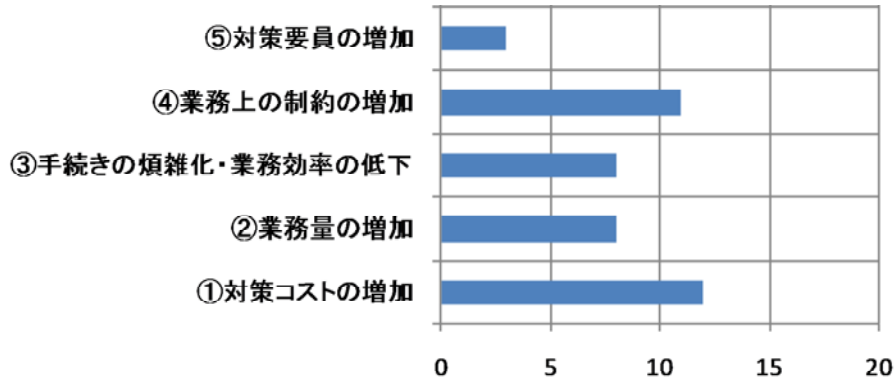


図 2.1-2 2005 年以降の情報セキュリティ対策の業務に及ぼした影響は？

セキュリティ対策による業務の効率低下の要因としては、「直接業務に無関係な依頼作業の増加」、「情報を利用・取得しづらくなった」という回答が多かったが、セキュリティ対策は業務上必要不可欠な手続きであるという意見が寄せられた[設問 1-3]。

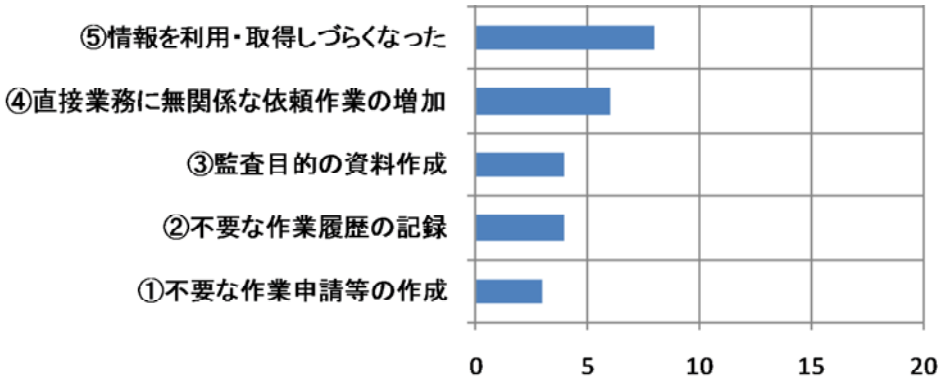


図 2.1-3 業務量の増加、業務効率の低下、業務上の制約の増加の要因は？

過去の ISMS 調査[8]でも、「情報資産の明確化と整理」、「社員意識の浸透と実践」上位に回答され、それと比べて、「セキュリティ事件・事故の減少」は少ない回答であった。これは、情報流出や漏えいという事象を事件・事故と認識していない、情報流出や漏えいの防止・軽減しても事件・事故は無くならない、という意見であると考えられる。

セキュリティ事件・事故に対する減少効果が少ないと感じる一方で、対策コストの増加と業務上の制約の増加を感じている。セキュリティ対策の向上と業務の効率化が相反する関係を示し、監査などの直接業務に無関係な依頼作業の増加し、情報の利活用に制約につながっている。それにもかかわらず、セキュリティ対策は企業イメージの向上・改善も含め業務上必要不可欠な作業として意識されているものと考えられる。

(2) 情報セキュリティ対策への組織幹部と従業員の認識

組織幹部の認識として、「コンプライアンス(法律)を重視」、「事業継続の重要課題と認識している」という回答が、「対策コストが高い」、「対策しても利益にならない」、「現場のリスクを理解していない」を大きく上回っている。一方、「現場のリスクを理解していない」組織幹部はいないという回答であった。

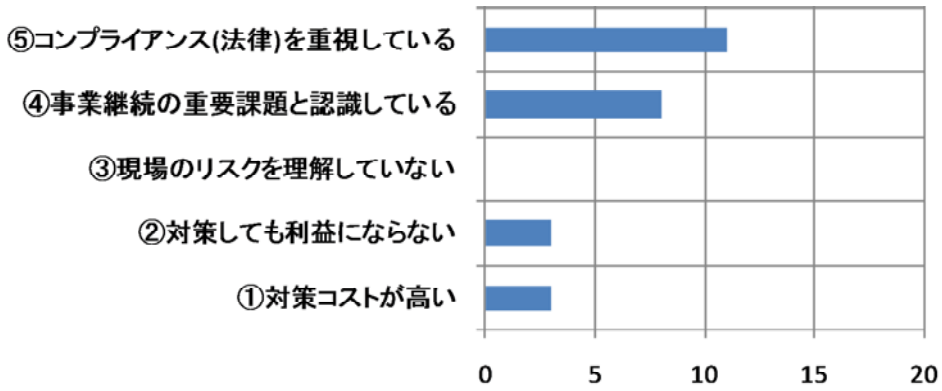


図 2.1-4 情報セキュリティ対策に対する組織幹部の認識？

回答者に占める情報システムベンダの割合が高いという要因もあるが、情報セキュリティ対策に対する組織幹部の認識は高いと考えられる。組織幹部は情報セキュリティ対策が必要不可欠であるが、直接業務に無関係な依頼作業の増加し、情報の利活用に制約が生まれ、コストが増大することに、これ以上の対策が打てないと考えられる。

従業員の認識についても、「情報セキュリティ意識が低い」、「自分の業務と合わない規則が多い」、「無関心・消極的」という後ろ向きの回答はほとんどない。研修等により、従業員の認識は全般的に高く、セキュリティ対策を重視しているという意見が多い。これに対し、4 分の 1 程度の少数意見ではあるが、「形式的な応対が多い」、「規則を知らない」と回答し、知識としての理解に止まっているケース、一部ルールや遵守事項が徹底できていない部分がある、という意見が寄せられている。

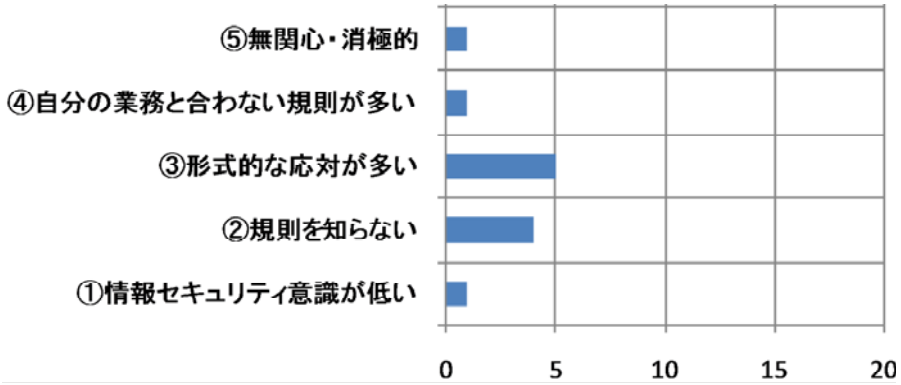


図 2.1-5 情報セキュリティ対策に対する従業員の認識は？

調査対象が ECOM 会員企業であり、情報セキュリティ対策に対する認識は組織幹部も従業員も総じて高いものであると考えられる。しかしながら、形式的な応対で規則を知らないなど、組織全体への徹底は十分であるとはいえない状況にあると考えられる。

(3) 今後の対策として必要と思う領域

情報セキュリティ対策として必要と思う分野については、「業務委託」、「社内（内部統制）」が半数を超える。基盤としては「企業内システム」をほぼ全員あげている。「企業間システム」、「家庭内 PC」、「クラウド環境」については 4 分の 1 程度の回答者が必要になると考えている［設問 1-7］。

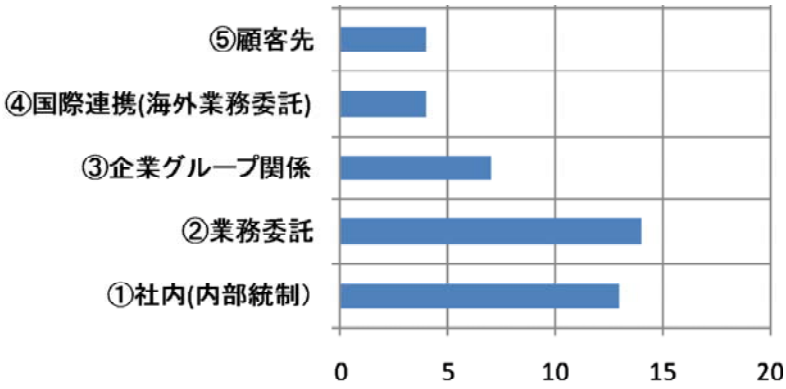


図 2.1-6 情報セキュリティ対策として必要と思う分野は？

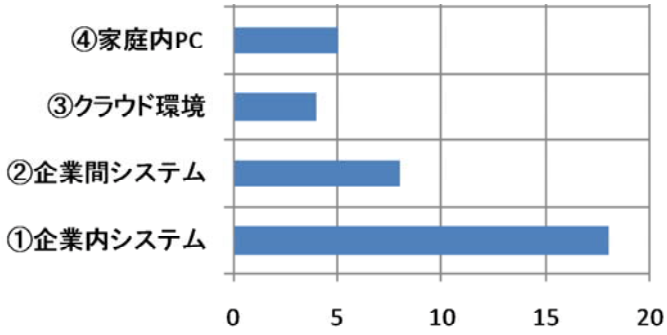


図 2.1-7 情報セキュリティ対策として必要と思う基盤は？

今後の情報セキュリティ対策への意見としては、形式にこだわらず、本来の目的、原点に帰った対策に重点をおけるような施策の実施（例、書式、多少の不備の容認など）、マネジメント的対策に加えた技術的対策の効果的適用拡大の検討、多数の委託先を抱える会社では目のなかなか行き届かない委託先のセキュリティの確保（担保）などが課題として挙げられた。

新しい情報犯罪の新しい手口が流行し、世間を騒がせる事件が継続して発生いる中で、自社の「企業内システム」のセキュリティを維持管理していくことで手一杯であり、昨今の景気低迷の状況下では、関連企業や取引先などの「企業間」まで手が回らない、「家庭内PC」のセキュリティを整備することや次世代の「クラウド環境」のセキュリティまで検討することを推進すべきであると回答できないというのが情報セキュリティ対策の現状と考えられる。

2.2.3. セキュリティ評価チャートの適用可能性についての回答

現在の対策状況に対して、セキュリティ事件・事故にはならなかったヒヤリ、ハットした情報管理と、セキュリティ評価チャートの適用可能性に対する回答内容を下記する。

(1) ヒヤリ、ハットした情報管理の存在、取り扱い、責任分界点

ヒヤリ、ハットした情報管理が程度あったか、という設問に対して、「時々ある」と「すこしあった」という回答を加えると半数程度に達する。一方、「頻繁にある」、「よくある」という回答は 0 であった。どのようなシーンで見かけられるという回答は「社内」が半数以上で、その他のシーンとしては、「業務委託」、「顧客先」が 4 分の 1 程度、「企業グループ」、「国際連携」は少数意見であった[設問 2-1]。ヒヤリ、ハットした事象で「頻繁にある」、「よくある」事象に関しては対策が施される。「時々ある」、「すこしあった」という事象をどのように抽出し、事前に対策を具現化していくか、が今後の課題と考えられる。

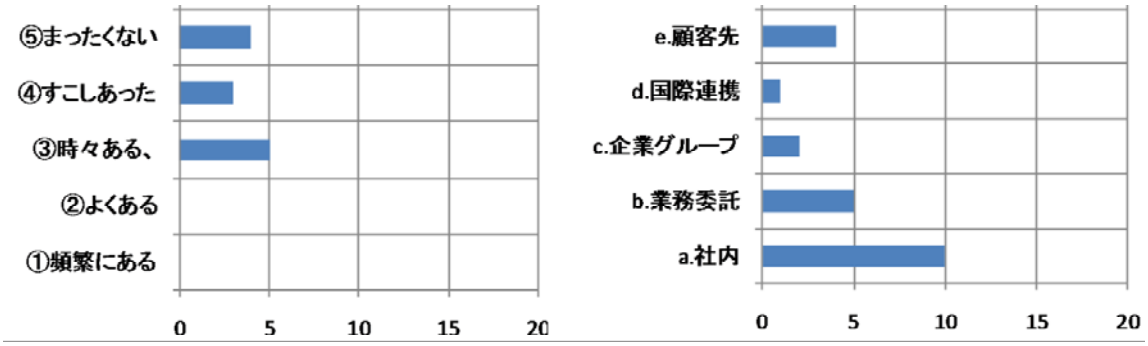


図 2.2-1 ヒヤリ、ハットした情報管理（受け渡しや情報格納）はあったか？

これに対し情報の取り扱いのフローは明確となっていたかという設問に対しては「周知徹底していた」、「取り扱いのフローはある」、「不明確だった」「意識していなかった」という 4 つの回答に分かれた[設問 2-2]。周知徹底していた、取り扱いのフローはあったにもかかわらずヒヤリ、ハットした情報の取り扱いになった原因や、取り扱いのフローを明確にできなかった原因を追及していくことが、情報セキュリティ事件・事故に繋がるヒヤリ、ハットした情報の取り扱いの改善につながるものと考えられる。

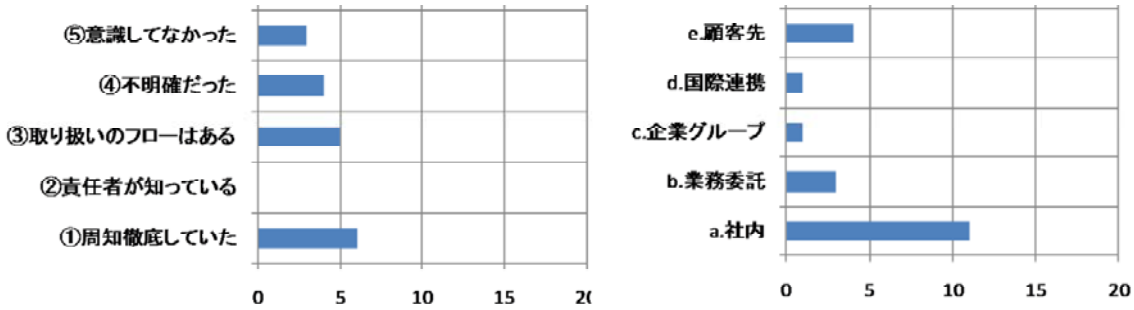


図 2.2-2 ヒヤリ、ハットした情報の取り扱いのフローは明確となっていたか？

(2) 機密情報の取り扱いの明確化と責任分担

機密情報の取り扱いに対して責任分界点は明確となっていたか、という設問に対しては、「関与者間で明確」、「不明確」という回答に分かれている。「部署間で決めている」、「管理者に任せている」、「意識していない」という回答は少数であった[設問 2-3]。関与者間で明確であっても部署間で決めていない、不明確であっても管理者に任せていない。これによって、機密情報でもヒヤリ、ハットした情報の取り扱いが発生しているものと考えられる。

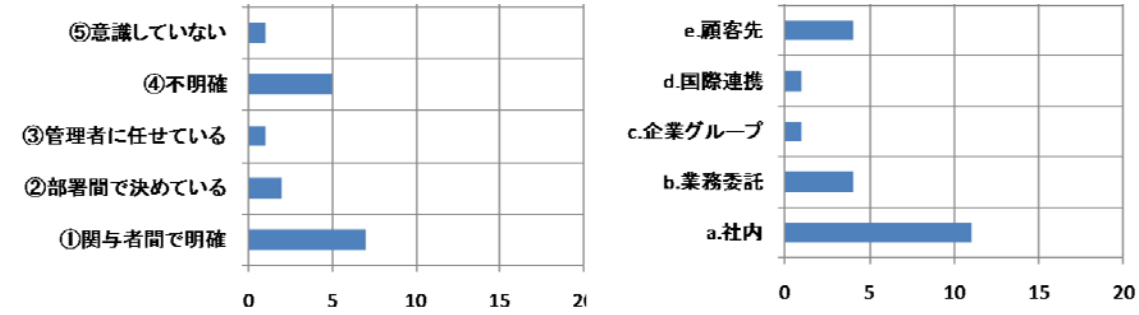


図 2.2-3 ヒヤリ、ハットした情報の取り扱いの責任分界点は明確となっていたか？

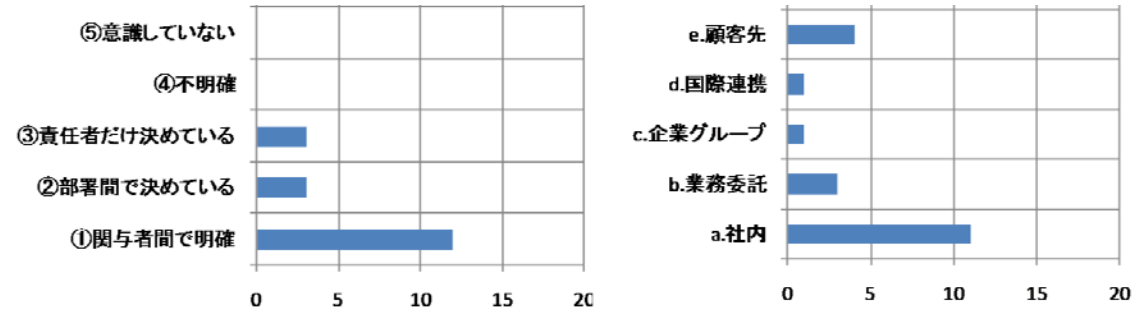


図 2.2-4 機密情報の取り扱いは関与者の間で責任分担が明確になっていたか？

(3) セキュリティ評価チャートの利用と標準化

情報取り扱いのセキュリティ評価チャートを見たことがあるか、という設問に対しては

「見ている」、「類似フローを知っている」という回答を合わせると、半数を超える。一方、「業務に使った」、「書いたことがある」という回答は少数であった。また、4 分の 1 の回答者は見たことがない、知らないという意見に対し、当社独自のフローを使用しているという意見もあげられた[設問 2-5]。

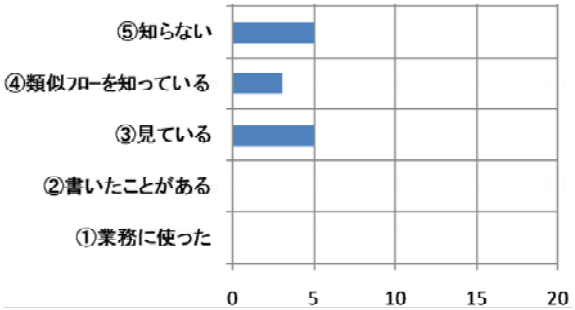


図 2.2-5 情報取り扱いのセキュリティ評価チャート を見たことがあるか？

セキュリティ評価チャートの標準についての設問に対しては、「あれば便利だと思う」という回答が半数を占める。「どちらともいえない」、「個別に決めるべき」という意見もある。また、定型的な業務には有効であるが、バリエーションのある業務に関しては有効性が不明という意見もあげられた[設問 2-6]。

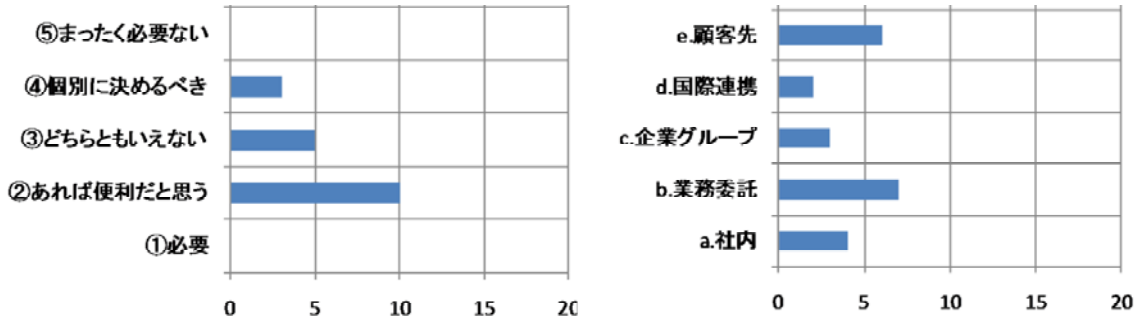


図 2.2-6 企業間利用でセキュリティ評価チャート の標準化をどう思うか？

WG メンバーの意見としては、個別の業務フローごとの作図のコストに対して責任分界点を明確にしたことによる効果がまだ見えていない、どのようなシーンに活用すべきであるか、効果の出るシーンに適用してその効果を広報することが重要といった意見があげられた。また、ISMS 認定制度やプライバシーマーク制度の評価項目に取り入れ普及させるなど、現在のセキュリティ対策プロセスの中に適用していくアプローチも必要であるという提案もあった。

本セキュリティ評価チャートに関する意見としては、「低コストで作成できるツール」、「記法の標準化やチャート作成の作業負荷対効果」、「評価チャートの独自性の尊重」、「不正競争防止法やプライバシーマーク制度の運用スキームへ活用する仕組み」、「チャートの作成業務の負担増」などを十分検討すべきであるという意見があげられた[設問 2-7]。

表 2.1 セキュリティ評価チャートへの意見

設問 2-7	意　　見
1.	・低コストで作成できるような、ツールが必要かと思います。
2.	・社内でリスク分析を行う際の前工程として類似のチャートを作成しているが、記法の標準化やチャート作成の作業負荷対効果について今後も検討が必要である。
3.	・あれば便利と思うが、各企業それぞれに独自性があることから、評価チャートについても個別にあるべきと思います。
4.	・個人情報は P マーク対応であり、企業機密管理は、社規等の規則や取引先との契約の中で対応している（問題があるとは思っていません)。 ・本件の如き評価チャートの標準化は、ECOM の活動範囲内では機能しないので、不正競争防止法(営業秘密管理指針）や P マーク運用などのスキームを活用する仕掛けがあった方が良いのではないか
5.	・セキュリティ評価チャートの利用は有効なところもあるが、チャートの作成が業務の負担増にならないように注意する必要があると感じます。
6.	・標準化を進める場合は、各企業の意見を基に十分検討していただきたい。

2.3. ヒアリング調査結果

2.3.1. 回答者の概要

金融、製造、システムベンダなどの企業担当者へ対象業界における一般的な情報の取り扱いについて、アンケート結果を踏まえ、本アプローチに関心があるアンケートの回答者や WG メンバーを中心にヒアリングを行った。ヒアリング先の業界を表に示す。なお、金融業は個人営業、電機は輸出と国内、印刷業は業界一般という視点で回答をいただいた。

表 2.2　業界別のヒアリング先

実施日	ヒアリング先
平成 22 年 1 月 22 日	金融業(個人営業)
平成 22 年 2 月　3 日	印刷業（業界全体)、電機（輸出）
平成 22 年 2 月　5 日	ソフトウェア開発・販売
平成 22 年 2 月　9 日	情報処理サービス、一般サービス業、化学工業、一般製造業、
平成 22 年 2 月 10 日	電機（国内）

2.3.2. 業務別の適用可能性について

各業界・企業の情報管理の実態からセキュリティ評価チャートの適用可能性と導入の可能性の視点から、13 社のヒアリング回答の内容を以下に示す。

(1) セキュリティ評価チャートの適用可能性(情報管理の実態)

各業界・企業の情報管理実態からの適用可能性としては、情報管理の責任分担、フロー図作成の有無、責任分界点の明確性と有効性、企業グループ相互の内部統制、業務委託・アウトソーシング、国際取引への適用の可能性として、設問とその回答内容を以下に示す。

(a) 責任分担

基本的に情報の受け渡し・情報格納については現場の管理となっているという意見が多い。機密レベルに応じて情報の取り扱い区分と責任者が定め、情報の受渡や保管の仕方はその責任者によって案件ごと定めているという回答がある。

表 2-3(a) 責任分担に関する設問と回答

設問 1-1	設問内容
実際に貴社で情報管理（受け渡しや情報格納）をする際に責任分担はどうなっているか？(現場か管理部門か) (例) ①社内データベースにある現場が収集した機密データの情報管理 ②社内データベースからダウンロードした機密データの情報管理 ③モバイルで社外に出たときの機密データの情報管理	

回答先	回答内容
金融業	・本社のデータベースにおいて一括管理し、そのデータベースに関してアクセス制限がある。ダウンロードするとダウンロードした側の責任となる。
印刷業	・組織ごとに、明確な責任分担を決めておらず、何か緊急事態の折には各部門責任者による委員会として対応している。
電機･輸出	・基本的には、情報管理者として、情報収集・発生の場である現場の責任となっている。
電機･国内	・情報の取り扱いについては、極秘、(秘)、社外秘などの秘密区分が定められており、部門毎に取り扱い責任者が定められている。 ・情報の受渡や保管の仕方は責任者によってプロジェクト毎に定められる。
ソフトウェア	・弊社において、情報の受け渡しに関しては、基本は現場管理となっている。 ・情報格納については機密情報管理システムが構築されており、情報の管理・格

開発・販売	納システムは、個人情報用とその他の機密情報用の 2 種類が提供されている。
情報処理サービス	・基本的に、情報の受け渡し・情報格納については現場管理となっている。但し、全体のデータベース管理やアクセス制限等については当然、管理部門が担当する。
一般サービス業	・情報の受け渡し・情報格納については現場でなく管理部門の一括担当となっている。
一般製造業	・基本的に、情報の受け渡し・情報格納については現場管理となっている。
化学工業	・基本的に、情報の受け渡し・情報格納については現場管理となっている。

(b)フロー図の作成

フロー図は作っていないという意見と、機密管理をしっかり実施している業務では、本アプローチのようなフロー図を作成しているという意見がある。特に、（ソフトウェア開発・販売）では管理システムによって、ワークフロー制御（承認プロセス、記録）も行っている。

表 2-3(b) フロー図の作成に関する設問と回答

設問 1-2	**設問内容**
現在、貴社で機密情報の取り扱いの全体フロー図もしくは個別の業務フロー図は作成されているか？	

回答先	**回答内容**
金融業	・すべての業務においてフロー図が作成されているわけではないが、業務手順として定義されている。
印刷業	・すべての案件に対して、全体もしくは個別業務のフロー図をおこしているのではなく、フロー図をおこす案件は限られている。
電機･輸出	・機密情報（個人情報含む）について、それがどこに保管され、業務上どう利活用されるかについてのフローが作成されている。
電機･国内	・機密情報を含む技術情報について、保管場所が定められ、業務上必要な場合は管理簿に記載して受け払いを確認している。すべてのプロジェクトでフロー図を作成するような管理は行っていない。
ソフトウェア開発・販売	・管理システムに、ワークフロー制御（承認プロセス、記録）が備わっているので、情報管理の全体のフローと言う意味ではツールで遵守が担保されている。 ・個人情報の取り扱いで業務委託が発生する場合には、個別にフロー図を作成し、その情報自体も管理項目の一部として管理ツールに登録することを義務付けている。

情報処理サービス	・会社全体のワークフローという点では、システム管理されているので基本的には、それでトータルの情報フロー図が備わっているのと考えられる。但し、個別の情報管理フローと言う点では、顧客情報等のお客様預かり情報以外には、個別にフロー図までは作成　していないとところが多い。
一般サービス業	・作業管理的なワークフローという点では、作業フロー図までしか作成できていない。
一般製造業	・作業管理的なワークフローという点では、フロー図が備わっているが、個別の情報管理フローと言う点では、フロー図までは作成していないところが多い。
化学工業	・個別の情報管理フローと言う点では、フロー図までは作成していない。

(c)責任分界点の明確性

詳細な責任分界点は事前に明確化されているというよりも、取り扱い責任者を決めておき、事後にその原因究明を含め、詳細な責任分界点の明確化を実施するという意見が多いように考えられる。

表 2-3(c) 責任分界点の明確性に関する設問と回答

設問 1-3	**設問内容**
万が一、受け渡しの途中に情報漏洩した場合に、情報の取り扱いの責任分界点は明確となっているか？	

回答先	**回答内容**
金融業	・責任分界点としては、データベースサーバ内までの情報は本社責任、アクセスしてダウンロードした時点でセールス責任となる。 ・オンザウェイで盗聴の場合にセキュリティパッチが不十分なことが原因での漏洩時だけがセールス責任となり、その他システム不良や man in the middle 等は本社責任となる。
印刷業	・基本的に情報の取り扱いの責任分界点は明確になっている。また情報の移送、送信手段も限定している。
電機･輸出	・情報漏洩については、その原因･過程について、誰のコントロール化にあったときの事故なのかを基準に責任分界点が明確になっている。
電機･国内	・情報漏洩した場合、その原因･過程については、定められた責任者によって明確化し、上長に報告する義務が課せられている。
ソフトウェア開発・販売	・個人情報の取り扱いについては、責任分界点は明確となっている。
情報処理	・重要機密情報（お客様預かり情報含む）は、責任分界点は明確となっているが、

サービス	一般的な社内情報等については不明確な部分がある。
一般サービス業	・一般的な社内情報等についてさえも不明確な部分がある。
一般製造業	・重要機密情報（個人情報含む）についても、一般的な社内情報等についても不明確な部分がある。
化学工業	・開発情報や一般的な社内情報等についても不明確である。

(d) 有効性

（印刷業）では、既にフロー図、リスク分析表の見本を掲載したガイドを発行している。（電機･輸出）では企業オリジナルなフロー図、（ソフトウェア開発・販売）では本アプローチとして採用したフロー図をすでに利用し、有効性を感じている。その他の意見も有効性があるという認識である。

表 2-3(d) 有効性に関する設問と回答

設問 1-4	**設問内容**
セキュリティ評価チャート は、機密情報の管理（受け渡しや格納）時に、社内の各部門間における責任分界点の検討に役立つと思うか？	

回答先	**回答内容**
金融業	・各セールスは、まるで現金を待ち歩いているような感覚でシビアに顧客情報を管理している。引き合い件名が増えるほど、漏洩リスクが高まるという恐れの中、日々移動の際に、不必要な用心とケアでセールス効率はダウンしている。 ・これらの業務改善などでフロー図を作ることは有効なのではないかと思う。
印刷業	・役立つと思うが、P マーク取得事業者の場合、審査機関である「日本印刷産業連合会」がフロー図、リスク分析表の見本を掲載した「印刷産業のための個人情報保護の手引き」という冊子を発行しているため、それと違ったフォーマットを使うことには躊躇する。
電機･輸出	・同チャートを使うと、機密情報のフローが明確になり、組織をクロスするときの送付元と受け取り先の責任が明確となり、各部門間における責任分界点の検討に役立つと思う。
電機･国内	・役立つと思う。
ソフトウェア開発・販売	・有効であると確信している。このチャートは弊社から事例として提示させていただいたものであるが、責任分界点というだけでなく、（業務の流れを容易に把握することができるので）効率化等の見直しにも役だっている。
情報処理サービス	・役立つと思う。

一般 サービス業	・役立つと思う。
一般製造業	・役立つと思う。
化学工業	・役立つと思う。

(e) 情報セキュリティガバナンスの内部統制

内部統制をおこなう上でも、本アプローチのようなフロー図があることが望ましいという意見が多い。その一方で、セキュリティ評価には、定性的な取り扱いのリスクだけでなく、「それぞれの事象に対しての発生確率（例えば、FAX を何枚送ったら、1 枚の誤送信をする可能性がある、という統計データ)」がないと可視化だけで終わる可能性があるという意見(印刷業)がある。

表 2-3(e) 情報セキュリティガバナンスの内部統制に関する設問と回答

設問 1-5	**設問内容**
セキュリティ評価チャート は、情報セキュリティガバナンスの内部統制という観点から有効なツールだと思うか？	

回答先	**回答内容**
金融業	・内部統制については、業界のガイドラインがあり、定められた業務手順を遵守することが重要である。
印刷業	・真剣に「評価チャート」を利用していこうと思った場合には、「それぞれの事象に対しての発生確率（例えば、FAX を何枚送ったら、1 枚の誤送信をする可能性がある、という統計データ)」が無いと、どこかで行き詰ると思う。
電機･輸出	・部門間における管理責任を明確にした上で、その組織相互の内部けん制機能という観点からも有効だと思う。また ISMS 等の監査においても、こういった第三者から見ても解りやすいビジュアルツールは評価されるポイントとなる。
電機･国内	・内部統制、財務諸表という観点では、担当部門（経理関連部署）でフローを検証し、幹部報告の上、取扱規則が決められる。現場（売上計上部門）には、データ入力時の規則として展開される。わかりにくい面もあるので、情報の流れを可視化したフローがあると理解しやすいと思う事がある。
ソフトウェア開発・販売	・情報セキュリティガバナンスの内部統制という観点から有効なツールではあるが、これだけで十分というものではないと考えている。有効度も情報の種類によって変化するものと思うし、たとえば、利用用途が限定されている個人情報についての有効度は、他の種類に比して高いものといえるのではないかと思う。
情報処理	・有効なツールであると思う

サービス	
一般 サービス業	・特に、顧客情報などの情報フローが作成できれば、有効なツールであると思う。
一般製造業	・特に、設計図面や試作品などの情報フローが作成できれば、有効なツールであると思 う。
化学工業	・きっちりと部門ごとに各種の情報フローが作成できれば、有効なツールであると思う。

(f) 企業グループ相互の内部統制

同じグループ企業内では同じ表現を利用することが望ましいという意見がある半面で、異なる組織間でも利用すべきであるという意見がある。

表 2-3(f) 企業グループ相互の内部統制に関する設問と回答

設問 1-6	**設問内容**
セキュリティ評価チャート は、企業グループ相互の内部統制という観点から有効なツールだと思うか？	

回答先	**回答内容**
金融業	・企業グループ相互の内部統制についても業界内で取り扱いルールが決められていると思う。
印刷業	・同一企業グループで同じ評価ツールを使って管理することは重要だと思う。
電機･輸出	・特に、様々な業種からなる企業グループの場合は、グループ間での共通のものさしが必要で、その意味でこういった評価ツールの存在は相互のセキュリティレベルの比較・牽制という観点からも役に立つ。
電機･国内	・企業グループ間としては、それぞれの企業グループが独自で実施しているので、同じ目線にすることは困難である。企業グループ内での企業間（関連会社）間では共通した情報管理に対する共通の表現があったほうが便利だと考える。
ソフト ウェア 開発・販売	・統一したルールとして合意の上の運用であれば、有効なツールであると思う。
情報処理 サービス	・有効なツールであると思う。
一般 サービス業	・関係会社間の顧客情報受け渡しに際して、有効なツールであると思う。
一般製造業	・関係会社間の情報受け渡しに際して、また共同開発作業時の責任分担の明確化

	として有効なツールであると思う。
化学工業	・関係会社間の開発情報等の受け渡しに際して、有効なツールであると思う。

(g) 業務委託、アウトソーシング

業務委託、アウトソーシングでは、委託元が委託先の管理監督責任を問われ、セキュリティ評価を SOW（Statement Of Work:業務仕様書）の一部として位置付けられるので、極めて有効であるという意見が大半を占める。

表 2-3(g) 業務委託、アウトソーシングに関する設問と回答

設問 1-7	設問内容
セキュリティ評価チャート は、委託業務やアウトソーシングという観点から有効なツールだと思うか？	

回答先	回答内容
金融業	・業務範囲外なので不明である。
印刷業	・委託元、委託先間で同じ評価ツールを使って管理することは重要だと思う。
電機･輸出	・当然、資本系列等のない企業間では、共通のものさしが必要性はもちろんのこと、特に委託元が委託先の管理監督責任を問われる、個人情報等の委託時にはさらなる評価･チェックツールとして有効に機能する。
電機･国内	・系列会社（1 次）では基本契約が交わされている。提供する情報は必要最小限に制限している。再委託先や関係先が数多くある場合にはフローを明確にする必要があると考える。
ソフトウェア開発・販売	・業務委託を行う上で、いわゆる SOW（Statement Of Work:業務仕様書）の一部として位置付けられるので、極めて有効であると思う。
情報処理サービス	・委託先管理が要求される場合は有効であると思う。
一般サービス業	・再委託先管理や孫受け先管理の手法として、有効であると思う。
一般製造業	・下請け管理の手法として、有効であると思う。
化学工業	・委託先の管理手法として、有効であると思う。

(h) 国際取引

製造業では、海外現地企業に対する部品加工依頼や業務提携作業が発生するケースなどでは有効であるという意見が多い。一方、海外企業が相手の場合、特に、当事者に情報管

理の意識のない状況では、国際規格としての ISO のような標準化・規格化がないと、評価ツールの作成合意をとることからは始めなければならない。国際取引では評価ツールの作成の動機付けが必要であるという意見がある。

表 2-3(h) 国際取引に関する設問と回答

設問 1-8	設問内容
セキュリティ評価チャートは、機密情報の受け渡しを伴う国際取引という観点から有効なツールだと　思うか？	

回答先	回答内容
金融業	・業務範囲外なので不明である。
印刷業	・国際取引についてはあまり検討できていない。
電機･輸出	･国際的な委託･アウトソーシング時にも､同様のことが言えるのはもちろんだが､海外企業が相手の場合､このような評価ツールの作成合意をとることから始めなければならない。したがって、国際規格としての ISO のような標準化・規格化が必要である。
電機･国内	・国内同様、提供する情報は必要最小限に制限している。海外企業が相手の場合、ビジネススタイルが異なり、このようなフローを明確にして、期日を決めて管理をするようなことを相互合意がとれるかは個々の企業では困難である。
ソフトウェア開発・販売	・あくまで当事者の情報管理意識が高いことが前提であるが、当該セキュリティ評価チャートは単なる取り扱いだけでなく、システム構築の要件定義の一部としても機能するため、有効と言えると思う。 ・当事者に情報管理の意識のない状況では、セキュリティ評価チャートを意識醸成のツールとして使えるが、これを以て情報セキュリティを担保するには、いささか力不足の感がある。
情報処理サービス	・オフショアでの海外現地企業にソフトウェア開発依頼等が発生するケースでは有効と言えると思う。
一般サービス業	・業務範囲外なので不明である。
一般製造業	・海外現地企業に対する、部品加工依頼や業務提携作業が発生するケースでは有効と言えると思う。
化学工業	・海外現地企業に対する、一部の材料調達や共同開発作業が発生するケースでは有効と言えると思う。

2.3.3. 各企業での導入の可能性について

各企業の現場に活用できるか、活用できないとしたら何か課題であるか、についてヒアリングを行った結果を以下に示す。

(1) 活用

各企業の現場での活用は、導入に対するコストと効果の不明であり、このままでの活用・受け入れは困難と考える企業と、既に個人情報を取り扱う業務で必須としている企業がある。また、全ての情報に対してフローを書くことは非現実的で、適用するシーンを絞るべきだという意見がある。

表 2-5（1）活用に関する設問と回答

設問 2-1	設問内容
現場でセキュリティ評価チャート（シート)を活用・受入れは実際問題として可能か？	

回答先	回答内容
金融業	・業務範囲外なので受け入れられるかは不明である。
印刷業	・実に重要だと思うが、それぞれの事象に対しての発生確率という統計データが加わってこそ完成すると思う。外部のアドバイザーのサポートも必要だと思う。
電機･輸出	・たまたま、当社では、同チャートと同種のフローチャートがすでに導入・運用されており、このままでの活用･受け入れは、困難と思われる。
電機･国内	・情報の機密レベルと取り扱う人の数が異なり、ケース by ケースだと思う。機密レベルと取り扱う人の数が多く、ルーチンワークとなるような取り扱いでは適用していく可能性はある。
ソフトウェア開発・販売	・弊社では、個人情報の取り扱いを業務委託する場合には、すでに必須条件としている。
情報処理サービス	・最終的に活用・受け入れは可能と思われる。
一般サービス業	・不可能ではないが、現状では困難
一般製造業	・不可能ではないが、かなりハードルが高い
化学工業	・不可能ではないが、その前に現場での情報セキュリティ意識の向上が前提である。

(b) 活用(導入)の課題

現場での活用が困難や不可能な場合、どうしたら活用・受け入れできるか？という設問に対しては、未導入の企業では、いきなり効果的なフローを書くことは困難で、ひな形の提供、外部のアドバイザーの支援、が必要という意見がある。また、情報セキュリティに関して、作業フローから情報フローへの意識改革が必要という意見もある。

表 2-5(b) 活用の課題に関する設問と回答

設問 2-2	設問内容
困難や不可能な場合、どうしたら活用・受け入れできるか？	

回答先	回答内容
金融業	・業務範囲外なので不明である。
印刷業	・外部のアドバイザーが必要だと思う。
電機･輸出	・回答 2-1 の事由（オリジナルな図の利用）により、現時点での受け入れは難しいが、国際標準化されて ISO のように規格化されれば、受け入れざるを得ない。
電機･国内	・ひな形が提供され、取り扱う情報や担当者を入力すれば作成と管理が容易となるようであれば可能性がある。
ソフトウェア開発・販売	・経験則から、業務委託等から導入するという方法がよろしいかと考える。
情報処理サービス	・前提条件としてこの評価チャートに対する現場での習熟と、類似の簡易フロー図等を既に導入しているところに対する、標準化等の働きかけが必要と思われる。
一般サービス業	・活用・受け入れのポイントは、顧客情報保護の大切さを含む、情報セキュリティ意識のさらなる向上が必要。
一般製造業	・活用・受け入れのポイントは、会社全体としての作業フロー意識から、情報フローの重要さへの意識改革が必要。
化学工業	・活用・受け入れのポイントは、会社全体としての作業フロー意識から、情報フローの重要さへの意識改革が必要。

(c) 他のツール

従来からシステムソフトウェアの開発でデータフロー、プロセスフロー、サービス品質を上げるためのサービスフローなどの図はある。情報セキュリティに関して、機密情報のライフサイクルをトレースするフロー図はなく、情報セキュリティ意識の高い企業では、オリジナルなフロー図を作成している。

表 2-5(c) 他のツールに関する設問と回答

設問 2-3	設問内容
責任分界点の明確化等の方策としてセキュリティ評価チャート(シート)以外で適切なツールがあるか？	

回答先	回答内容
金融業	・特になし。
印刷業	・責任分界点の明確化だけで考えれば、契約書、仕様書、発注書が基本と考える。
電機･輸出	・回答 2-1 で回答の通り、当社オリジナル仕様ではあるが、同様の目的で、同様のツールを実際に運用している。
電機･国内	・システム・ソフト開発では業務フローを記述することは SE であれば当たり前のように行っている。システム・ソフトの動作記述ではなく、機密情報のライフサイクル（発生から消滅まで）を中心したフローについては不知である。
ソフトウェア開発・販売	・特に思い当たらない。
情報処理サービス	・業務フローチャート図や作業単位規約等
一般サービス業	・特になし。
一般製造業	・特になし。
化学工業	・特になし。

2.4. 実態調査のまとめ

アンケート結果とヒアリング結果を業務データプロセスセキュリティ評価チャート（情報セキュリティの見える化）の視点から、情報セキュリティ対策の実態とセキュリティ評価チャートの適用可能性を考察する。

2.4.1. これまでの情報セキュリティ対策の効果

この 5 年間に個人情報を中心として情報セキュリティ対策が行われ、情報資産の明確化と整理により、情報流出や漏えいの防止・軽減や社員意識への浸透と実践が進んできた。その一方で、対策コストと業務上の制約が増加し、直接業務に無関係な依頼作業と情報の

利用・取得の困難性が増加し、業務の効率低下が起こっている。

情報流出や漏えいの防止・軽減にはつながっていても、実際に起こるセキュリティ事件・事故への減少効果は少ないと感じ、対策コストと業務上の制約の増加があっても、セキュリティ対策による企業イメージの向上も含め、業務上必要不可欠な作業として意識されているものと考えられる。

金融業の現場コメントを借りると、各セールスマンがまるで現金を待ち歩いているような感覚でシビアに顧客情報を管理して、引き合い案件が増えるほど、漏えいのリスクが高まるという恐れの中、日々の活動や移動の際に不必要な用心とアフターケアで業務効率が低下する、というのが現在の情報セキュリティ対策の実態であると考えられる。

2.4.2. セキュリティ評価チャート導入への課題

今日のセキュリティ対策では、企業の事業責任から、情報セキュリティに対するコンプライアンス(法律)と事業継続を重要課題として認識し始めている半面、直接業務に無関係な作業の増加、情報の利活用制約の発生、対応コストの増大により、これ以上の対策は打ちたくないと感じ始めている。

一方、先進的な企業では、個々の作業の中で直接業務に無関係な作業の増加を増加させるのではなく、機密情報のライフサイクルの中で必要とされる情報セキュリティ対策の責任分界点を明確化させ、それぞれの組織が実現できるセキュリティ対策の責任分担により、効率的な業務を遂行しようとしている。

今回の実態調査でも、情報セキュリティの責任分界点と責任分担を明確化し、効率的な業務を遂行しようとするセキュリティ評価チャートのアプローチを有効と考える意見は多い。しかしながら、現実問題として、現場への本アプローチの導入がさらなるコストの増大につながるのではないかと、懸念している。

現場でセキュリティ評価チャートを適用していくコストと、必要とされる情報セキュリティ対策の責任分担により業務が効率化するコストに着眼して、適用するシーンを考えていくことが必要である。

(1) 内部統制への適用

内部統制をおこなう上でも、本アプローチのようなフロー図があることが望ましいという意見がある。これらの多くは、フロー図を作成することは情報セキュリティがシステム部門や機密情報管理責任者だけの責任でなく、現場（業務部門）の担当者にも責任分担を追っていることを明示化することに繋がる。

内部統制に対して本アプローチは、担当者も含めた全体での責任分担が明示することによって、責任者や担当者の管理ミスや不正操作を抑止することを期待するものである。本アプローチの適用は、これまでのセキュリティ対策で決めた数多くのルールを周知徹底させるコストと、各自がビジネスの源泉として利用する機密情報のフローに関わるルールを

周知徹底させるコストとを比較し、どちらが効果的であるかという事を判断する必要がある。

なお、第 3 章で、企業内での複数の部署における個人情報の取り扱いに関して、情報のフローを変えることによって、個人情報に関わる取り扱いの作業コストを削減する事例を示す。

(2) 企業グループ統制

同じグループ企業内では同じ表現を利用することが望ましいという意見がある半面で、異なる組織間でも利用すべきであるという意見が挙げられている。グループ企業内でも同じ事業ミッションを背負っているわけではない。事業とする製品やサービスを提供していく上で、営業（法人・個人）、開発、製造などの異なったミッションを持っている。異なるミッションをもった組織間でも共通理解ができる表現を実現していくことが必要である。

(3) 業務委託・アウトソーシング

2007 年より委託元が委託先の管理監督責任まで問われるようになり[9,10]、自社から情報漏えいを起こさなければ、情報セキュリティに対する責任を問われないフェーズから、業務を委託した関係先での情報漏えいに関しても責任を問われるフェーズに変わってきている。

先進企業では既に、セキュリティ評価を SOW（Statement Of Work：業務仕様書）の一部として位置付け、委託契約書の中で情報セキュリティの責任分担を定めている[11]。本アプローチのスタート時にはどのようにフロー図をどのように作図するかについて苦労があったが、普及活動を行い、作図することの合意形成がなされてくると、委託先からセキュリティ対策を逆提案され、委託元と委託先でコンセンサスのとれた効率的な業務へと進化している。

特に、個人情報を取り扱う業務ではフロー図の作成が義務付けられ、委託先の選択、契約の締結、委託先の監督というプロセスの中で管理業務の効率化とともに、委託元と委託先での必要となる情報セキュリティ作業の最適化が進み、業務に無関係な作業の削減につながっているものと考えられる。なお、第 3 章では、業務委託の例をあげ、本アプローチの有効性を示す。

(4) 国際連携

この 5 年間の情報セキュリティ活動では、個人情報保護を中心とした活動が行われてきた。ヒアリング結果でも、金融業と製造業では情報セキュリティ対策の対象が異なっている。金融業は個人情報、製造業では仕様書や設計図面等の技術情報に着目している。日本の製造業の多くは海外生産・調達・開発などの国際連携を必要としている。

製造業で、海外現地企業に対する部品加工依頼や業務提携作業が発生するケースなどで

は本アプローチが有効であるという意見が多い。しかしながら、ISO のような標準化・規格化がないと、情報セキュリティに関するフロー作成の合意をとることからは始めなければならない。

3. 情報セキュリティの見える化

― 業務データプロセスセキュリティ評価チャート作成マニュアル ―

3.1. セキュリティ評価チャートの使い方

本セキュリティ評価チャートは異なる文化を持った企業間や異なる専門性や目的をもった部署（法務部門、資材・調達部門、業務部門、システム部門）間の情報の取り扱いに対する責任分界点を定めリスク対策の責任分担のコンセンサスを得るために用いる。本チャートの使い方を、図 3.1 の個人情報にかかわる業務委託の例を用いて説明する。

3.1.1. 個人情報保護ガイドラインの改訂

2005 年の個人情報保護法の施行を受けて、大企業を中心に情報セキュリティ対策が進み、対策を行った企業情報システムやその職員からの情報漏えいは減少傾向にあるものの、委託先企業や派遣職員などからの情報漏えいがいまだに絶えない状況にある。

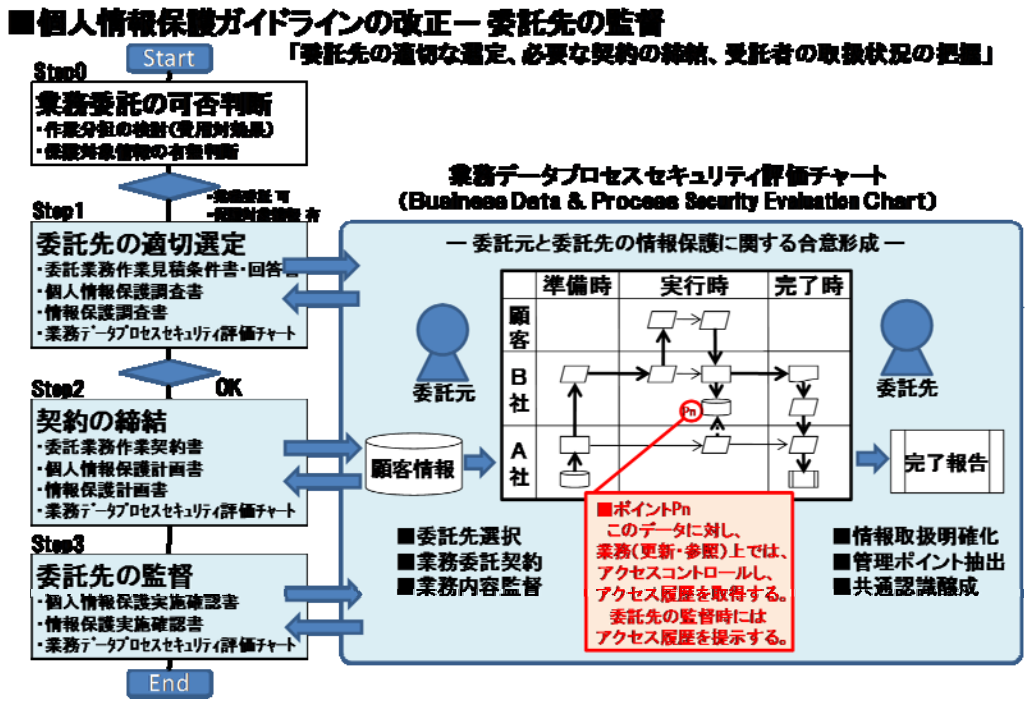


図 3.1. 業務データプロセスセキュリティ評価チャートの利用例

経済産業省は、一般産業での個人情報の取り扱いにおけるガイドラインを改訂して、2007年 3 月に、情報保護に対する業務委託先の適切な選択、適切な契約の締結、委託先での情報の取り扱いに関する監督を行うこと[9]、2009 年 10 月には委託作業を透明性を確保することが追記された[10]。

3.1.2. セキュリティ評価チャートの利用

この改訂により、個人情報保護の観点から、委託元企業は委託先企業を適切に選定し、契約を締結、委託先での取り扱いを監督することが必要となっている。そこで、この企業間や組織間での情報の取り扱いにかかわる情報セキュリティの責任分界点や責任分担を明確にするセキュリティ評価チャートを利用する。

(1)チャートの作成

個人情報の受け渡しから委託業務完了報告までの間に行う、情報の収集・保管・受け渡し・利用・破棄等の処理を記載したチャートを作成する。

(2) 委託先の適切な選定での利用

作成したチャートを用い、委託先企業での情報保護対策をヒアリングし、その内容を評価し、適切な委託先を選定する。

(3) 機密情報保護契約の締結

委託業務先の情報保護対策とチャートを契約条件として添付し、機密情報保護契約を締結する。

(4) 委託先業務の監督

個人情報の受け渡しから委託業務完了報告までの間、契約書に添付したチャートと情報保護対策が履行されているか、の監督（現場視察や報告書確認）を行う。

3.1.3. チャートの効果

委託先の適切な選定から委託先業務の監督を行う過程において、チャートを利用することによって、責任分界点とリスク対策の責任分担が明確化され、それにかかわる関係者間での明確なコンセンサスが得られ、実行性のある対策が確実に実行されるようになる。

(1) チャートの作成

作業発注者自身が業務データとプロセスの流れが正確に把握できる。

(2) 委託先の適切な選定での利用

委託候補先の具体的な情報セキュリティ対策の内容を評価することができる。

(3) 機密情報保護契約の締結

委託先のみならず、委託元の法務部門、資材・調達部門、業務部門、システム部門などとの合意形成ができた機密情報保護契約の締結ができる。

(4) 委託先業務の監督

具体的なチャートを基にした現場視察や報告書確認により確実な監督ができる。

3.2. セキュリティ評価チャートの書き方

前述のような効果を出すにはチャートの書き方が重要なポイントとなる。機密情報として押さえるべき情報の取り扱いの記載をもらさず、可読性の観点から詳細化しすぎず、記載する必要がある。また、異なる企業間で使う、分野の異なる専門家（法務、調達、業務、システム管理など）とのコンセンサスを得るという観点から、相互で理解できる標準的な記述形式を利用することも必要となる。

本チャートでは、情報セキュリティの責任分界点を明確化するということに焦点を当て、保護すべき情報のステークフォルダー（情報主体、委託先企業、委託元企業など）と、情報の準備、利用、完了のフェーズに分けて情報の取り扱いを記載する。以下では、記載内容と記述形式を説明する。

3.2.1. 記載内容

チャートの記載内容は、電子化された情報の流れとその処理（電子的な取り扱い）だけを書くというものではなく、紙などを用いた情報の受け渡しや人手で行う作業（現物的な取り扱い）についても記載する。なお、電子的な取り扱いと現物的な取り扱いはリスクが発生する特徴、情報が漏洩する規模、情報セキュリティ対策などが異なるため、表記を変えて記述する。

機密情報にフォーカスするという観点から、機密情報の発生から消滅までに行われる電子的な取り扱いと現物的な取り扱いを記載する。本チャートでは、機密情報保護に焦点を当て、機密情報を含まない情報の流れや処理については詳細に記述しない。情報システム構築のデータフローが実行するデータや処理を網羅的に記述するのに対して、本チャートでは、機密情報にアクセスする取り扱いを網羅的に記述していく点が異なる。

それぞれの記述内容に対する記述形式を以下に示す。

3.2.2. 記述形式

(1) 情報の取り扱いの記述

本チャートは下記の取り扱いに分けて、オブジェクトごとに標準的なシンボル（表記方法）を利用して記述する。標準的なシンボルを図 3.2 に示す。

(i) 情報処理	シンボル	(iii) 情報と処理の流れ	シンボル
・自動処理		・電子的情報の流れ	
・人的処理		・現物的情報の流れ	
・確認処理		・閲覧・確認の流れ	
		・業務処理の流れ	

(ii) 情報格納	シンボル	(iv) 情報保護の	シンボル
・電子的格納		・管理ポイント	
・現物的格納			

図 3.2. 評価チャートのシンボル

(a) 情報処理

・計算機処理：計算機で行われる処理
（人手を介さない処理）

・人的処理：人手で行われる処理。
（計算機を使用しても、人が機密情報を見る場合は人的処理とする）

・確認処理：機密情報の取り扱いを確認する処理
（実行時や完了時の機密情報取り扱い(複写、破棄等)の報告）

(b) 情報格納

・電子的情報格納：電子化した情報の格納
（サーバーのデータベースや PC のファイルなど、
電子的な記憶媒体で自動的に受け渡しがトレースできる情報格納）

・現物的情報格納：現物による情報の格納
（紙、CD、DVD、USB などの物理的媒体で、自動的に受け渡しがトレース
できない情報格納）

(c) 情報と処理の流れ

・電子的情報の流れ：電子化した情報の流れ
（電子メール、Web などによる情報の受け渡しの方向）

・現物的情報の流れ：現物による情報の流れ
（紙、CD、DVD、USB などによる情報の受け渡しの方向）
・業務処理の流れ：計算機処理、人的処理などの流れ
（計算機処理、人的処理などの業務処理の順序）
・閲覧・確認の流れ：格納情報の閲覧・確認の流れ
（格納情報に対する閲覧・確認のためのアクセス）

(d) 情報保護のタイミングと対象

・管理ポイント：情報保護を必要とするタイミングと対象の指定
（誰が、どの情報に対する取り扱いについて管理するかのポイント）

(e) その他

・シンボルには関与者の間で理解容易な業務用語で名前をつける。
・管理ポイントは英記号名など ID を付け、別表にその内容を記載する。
・本書に準じない形式には必ずその意味を注意書きとして記載する。

3.2.3. 評価チャートのフォーマット

評価チャートを記載するフォーマットを図 3.3 に示す。

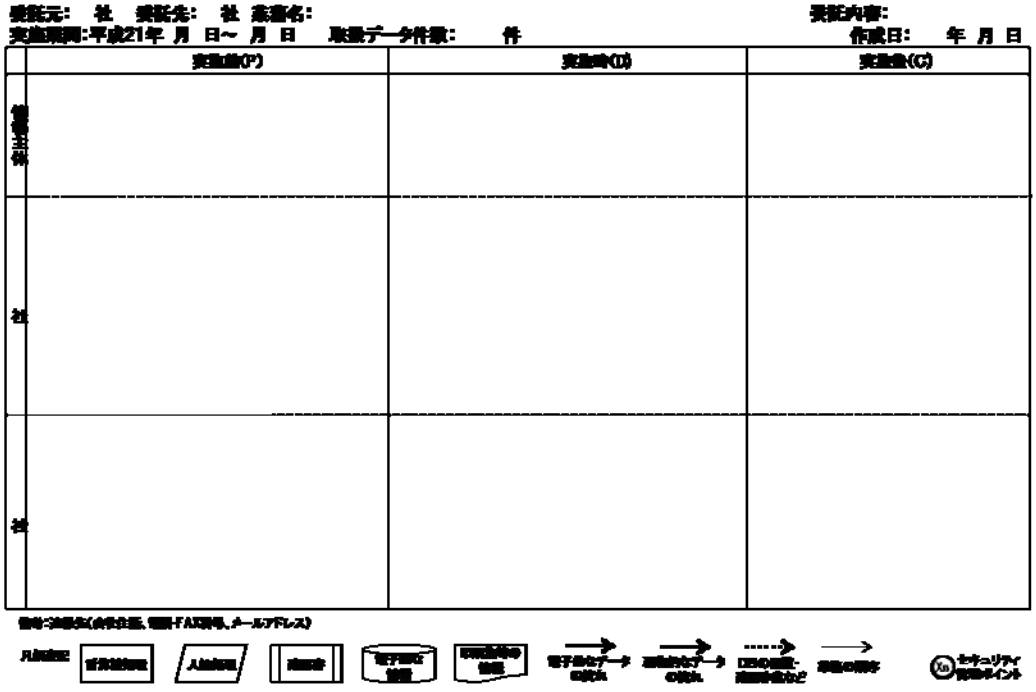


図 3.3. 評価チャートのフォーマット

(a) 概要(ヘッダー)の記載

評価チャート記載内容の概要として下記の項目などを記載する。

・業務名、作業内容、実施機関
・実施期間、取扱データ(機密情報)の件数、作成日・承認日

(b) 内容の記載

縦軸は機密情報のステークフォルダー、横軸に取り扱いのフェーズ分けを記載する。

・縦軸：情報主体者、実施機関（顧客窓口、サービス提供者、など）

・横軸：実施前(計画・準備）、実施（作業実行)、実施後（完了報告など）

(c) 注意書き(フッター）の記載

注意書きとしては使用したシンボルとその意味を記載する。

3.3. 使い方の例

本評価チャートの使い方として、事例 A は組織内での個人情報取り扱い業務改善、事例 B は業務委託の管理ポイント抽出、事例 C は技術情報取り扱い業務改善を示す例である。

これらの例では、業務のデータとプロセスのフローを作成し、その記載内容を追加、修正しながら、その中に含まれるリスクを評価して、担当者間、部署間、組織間での合意形成を行っている。事例 A では企業内での取り扱いの改善を行い、事例 B では企業間での合意形成により委託業務の監督の視点（管理ポイント）を決め、事例 C では技術情報の取り扱いに関して評価チャートの記述方法を改善し、技術評価の業務自身を改善した例である。なお、事例提供者の守秘義務上、以下では、組織名や対象情報などは仮名とした。

3.3.1. 委員会設置から謝金支払・報告書配布(事例 A)

A 社の各部署では 20 名程度の社外委員を招聘して、製品規格審査などの委員会を年間数回開催し、報告書を作成している。これまで、社外委員の委員委嘱、謝金支払を総務部門が一括して取り扱ってきたが、2005 年より社外委員の個人情報の取り扱いを各部署の主席研究員に任せるようになった。図 3.4 に委員会設置から謝金支払・報告書配布までの業務データプロセスフローを示す。まず、主席研究員が持っている名刺 DB から今回の委員会の趣旨に合わせて、委員を選び内諾を得る。総務に委員依頼の了解を採り、依頼書と引受書を送付する。社外委員は引受書に謝金受取の口座番号を記載し、主席研究員に送る。主席研究員は全員の引受書を集め、四半期ごとに謝金支払のために、経理へ提出する。

2005 年の個人情報保護法により、個人情報取り扱い事業者として、紛失などが起こると事件扱いとなるため総務での一括管理をやめ、主席研究員個人責任の上、まとめて引受書を経理が受け取る形にしたものである。このため、主席研究員は社外委員からにバラバラに送られてくる引受書を受け取り、委員費支払いまでの約 3 ヶ月間、口座番号が記載された引受書を机の引き出しで保管していた。下記の例（朱記)、社外委員が郵送してから、経理が保管管理するまで、3 ヶ月近く口座番号が記載された個人情報が企業の中で滞留している。このリスクを明示的に示し、総務・総務での一括受付として例が、図 3.5 の例である。

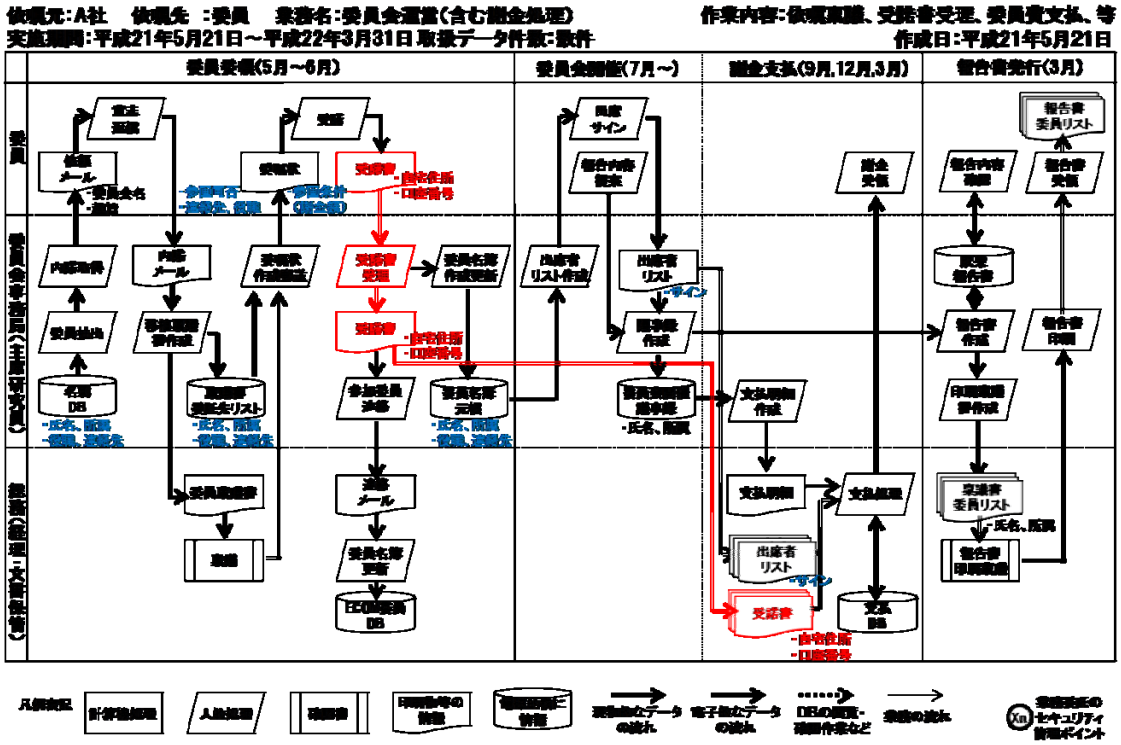


図 3.4. 委員会設置から謝金支払・報告書配布までの業務データプロセス(事例 A)

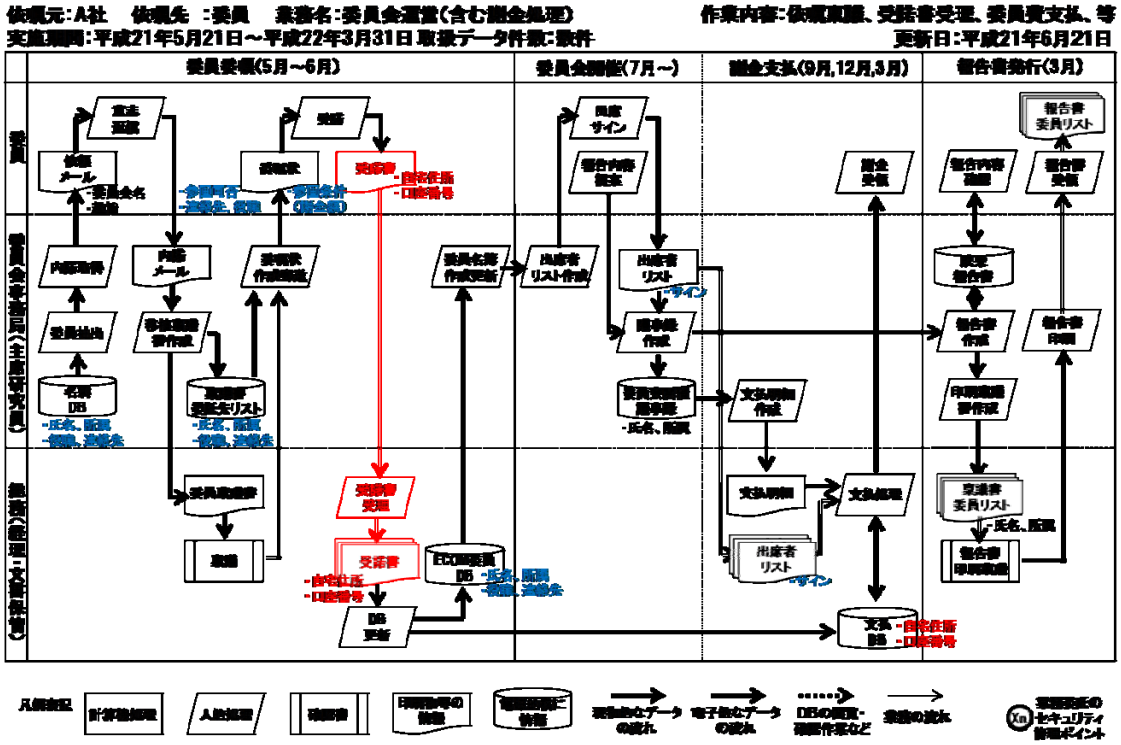


図 3.5. 組織内での業務改善(事例 A)

3.3.2. 商品説明会(イベント)参加者募集から参加者報告の業務委託(事例 B)

A 社の広報部では毎年 1,000 名程度の参加者を集め、商品説明会を開催している。これまでの参加者は 5,000 名を越える。5 名の広報部員では、商品説明会を運営しきれないので、イベント会社の B 社に参加者募集、参加登録、登録証の発行、商品説明会の運営を業務委託してきた。これまでは、広報部では、約 5,000 名の既存参加者リストを B 社に渡して一括して作業を頼んでいた。

2005 年の個人情報保護法により、B 社が 5,000 名以上の個人情報を保有すると個人情報取り扱い事業者となる。A 社の社内基準では、プライバシーマーク認定取得事業者しか業務委託できない。これまで委託していた B 社に業務委託できず、新しい委託先とイベントの手順、コンテンツの作成などを打ち合わせしていては会期に間に合わない。既存参加者への案内は A 社からメールで直接発信することとし、B 社には、Web 上に参加者登録サイトを開設して、約 1,000 名の参加者登録を受け付け、商品説明会のまでの準備作業、を業務委託することとした。

これまで、既存参加者情報は守秘義務契約を交わし、B 社の管理責任として業務委託を行ってきたが、2007 年のガイドラインの改定により、A 社の委託先の適切な監督が必要となった。そこで、フローを作成し、委託先との打ち合わせを行った。作成したフローを図 3.6 に示す。この図を用いて、責任分界点と管理ポイントを話し合い、管理ポイントにおける情報の取り扱いを作業契約として明記することとした。管理ポイントを図 3.7 に示す。

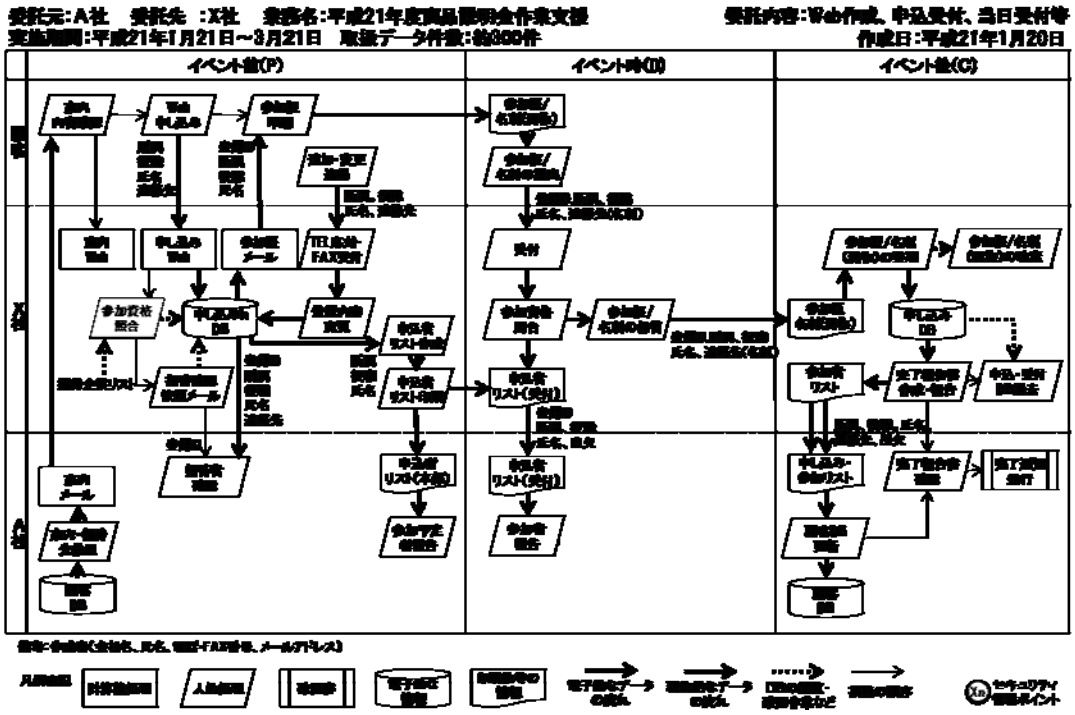


図 3.6. 商品説明会（イベント）参加者募集から参加者報告の業務委託(事例 B)

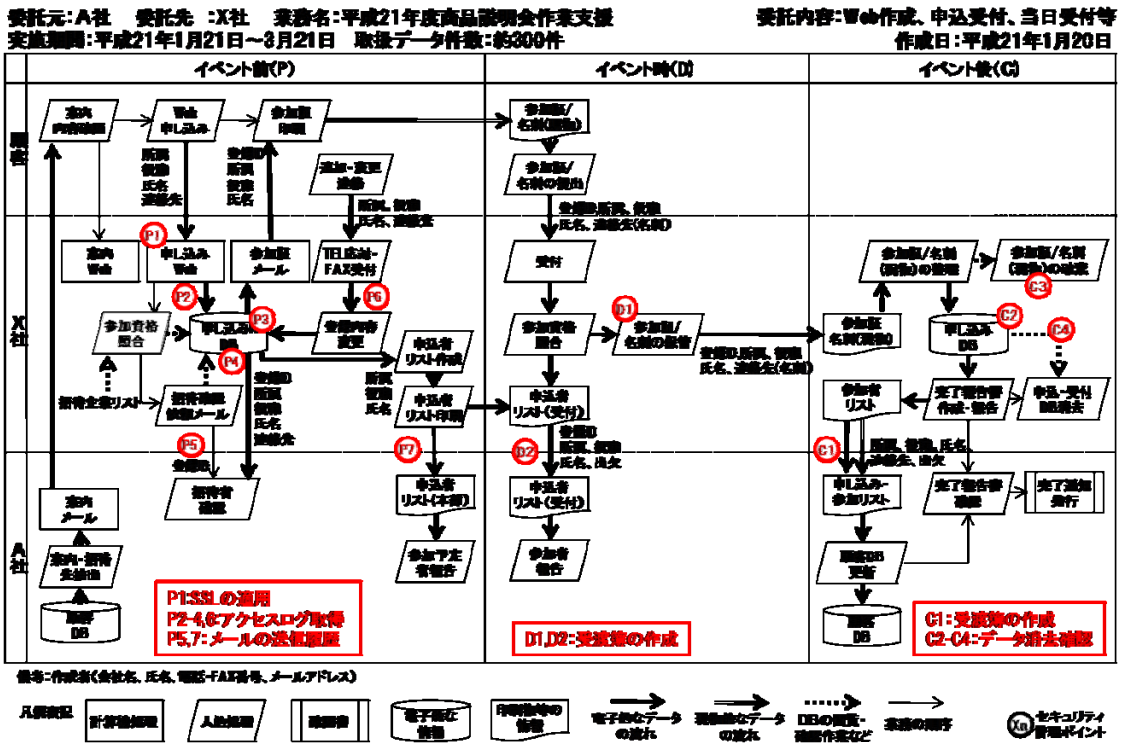


図 3.7.事例 B の業務委託時のセキュリティ管理ポイント(事例 B)

3.3.3. 入札時の技術審査フローの記述と業務の改善(事例 C)

A 社は複数の部品会社から技術情報と価格を入手し、社内外の専門家（評価委員）に評価を依頼し、技術審査を行って、購入する部品を決定している。専門家の評価には、詳細な技術情報を必要とし、部品会社にとっては死活問題となる技術情報である。そこで、A 社の入札担当者は入札時の技術審査の業務データプロセスのフローを作成した。作成したフロー図を図 3.8 に示す。縦軸は、評価委員、入札部署、部品会社とした。公募に応募した部品会社にメールを送り、部品会社から送られてきた資料を複写し評価委員に渡す。入札担当者は、評価委員から評価結果と配布した資料を回収して、回収した技術資料を滅却する。

情報管理として重要な機密情報は技術情報であり、その主体者は部品会社である。そこで、縦軸を部品会社、入札部署、評価委員とし、機密情報である技術情報を中心として書き直した。書き直したフロー図を図 3.9 に示す。評価委員を中心にしたフロー図から、技術情報を中心とした図に書き直すことによって、機密情報である技術情報の受け渡しの際に確認すべきことやエビデンス（証拠）として残すべき書類が明らかとなった。

これによって、技術情報の受領書、返却確認書などの帳票を作成して、組織間での情報の受け渡しとその間の責任の所在を明確にした。従来、評価委員の方に気を使っていたが、フロー図や受け渡しの帳票を使って審査の流れを説明することによって、手順が明確となり、評価委員の方々も技術情報の受け渡しを正確に行えるようになった。

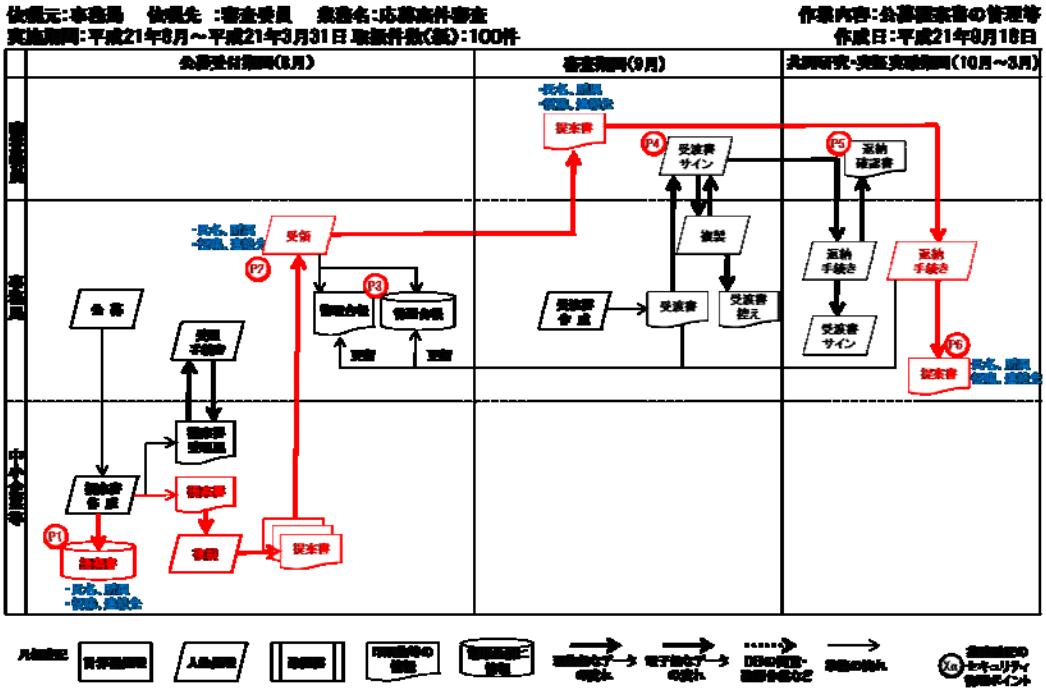


図 3.8. 技術情報の公募から審査終了までの業務データプロセス（事例 C）

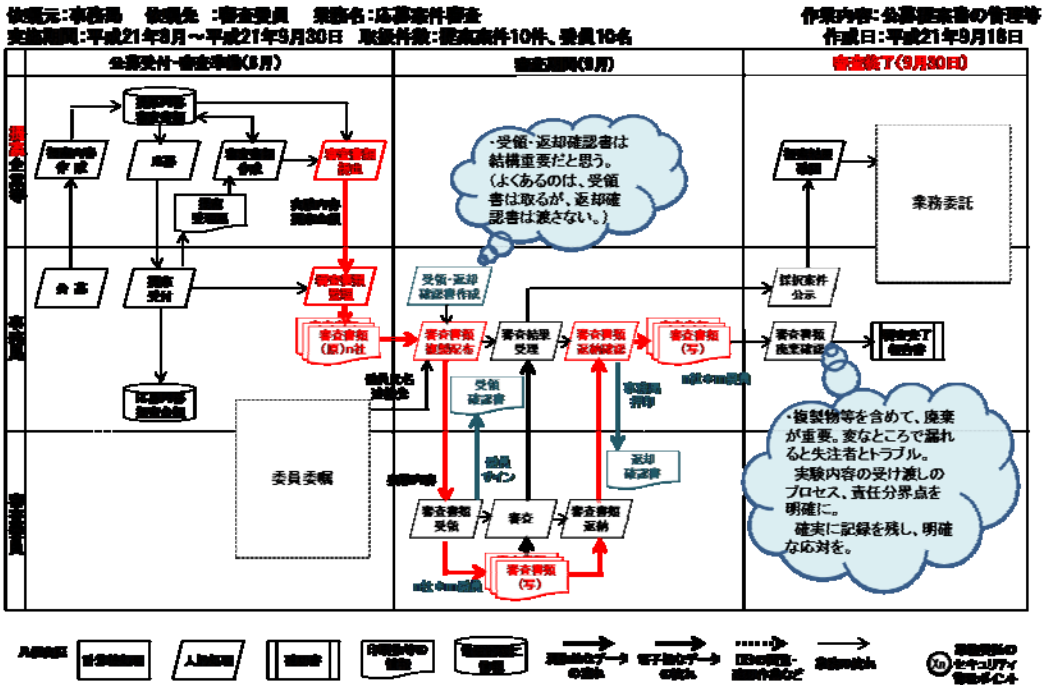


図 3.9. 事例 C の記載方法と業務の改善

3.4. 書き方のノウハウ

このアプローチは、書き方や使い方に正解があるという事でも、本ガイドの表記や手順に必ず従わなければならないという事でもない。重要なポイントは、内容を付け加えながら、関与者と合意していくことである。はじめから正確で詳細なフロー図を書く必要はない。詳細なフロー図はかえって押し付けとなる。自分のわかる範囲でしっかり管理しないと危ないと思う機密情報を、発生から消滅までの取り扱いを追いかけ、自分のわかる範囲で作業や受け渡しの仕方を記載し、関与者と話し合い、存在するリスクやその対策の責任分界点や責任分担の透明性を高めていくことが重要な点である。

初めて書くときにはいろいろな隘路の迷うことがあるが、2、3 枚のフロー図を記載するとだいぶ書き方がわかってくる。最終的には、社内の法務部門、システム部門などの異なる組織の人が見るということを意識して記述することが重要である。

(1) 機密情報の選択

このフロー図では機密情報が発生してから消滅するまでのフローを記載する。たくさんの機密情報を記載しようとすると複雑になる。まず、もっとも重要な機密情報を選択する。特に部署内の担当者間、社内の部署間、企業間で受け渡しが行われ、その責任の所在を明確にしないと、自分がその責任を取らされるものを選択する。管理が不明確で、危ない不安な情報であればあるほど、書き終わったときには頭の中がすっきりする。

(2) 縦軸と横軸の仮置き

縦軸は機密情報の主体者を上とし、その情報から遠い存在を下に配置する。また、横軸はその機密情報を利用するフェーズを中心におき、はじめにやるべき機密情報の収集などの準備フェーズや機密情報を使い終わって破棄したかなどの確認フェーズを必ず配置する。

(3) 発生と消滅のオブジェクトの記載

書き始める際には、まず機密情報の発生の情報格納や情報収集の作業を準備フェーズに置き、最終的に消滅を確認する確認処理や廃棄処理などを記載する。この発生と消滅のオブジェクト（データ格納と作業プロセス）を記載したら、その間を、情報の取り扱いと受け渡しのオブジェクトでつなげることでフローが完成する。

(4) 情報の取り扱いと受け渡しのオブジェクトの抽出

同じ人が取り扱う処理はなるべく大きな単位でオブジェクトを抽出する。逆に、受け渡しはなるべく詳細に記載し、受領書などのエビデンスも記載する。また、複数の人がアクセスする情報は誰が何の処理をするためにアクセスしているかがわかるように記載する。

(5) 現物的なオブジェクトと電子的なオブジェクトの切り分け

人的処理と電子的処理、現物的な流れと電子的な流れの切り分けに悩むことがある。基本的な考え方は、電子的処理は人が介さず計算機が制御して行う処理とすることである。また、電子的な流れとはメールなど電子的に制御され、必要に応じて暗号対策や履歴が取れる流れである。したがって、電子的なデータであっても対策などの施されていない USB、CD を用いた流れは現物的な流れになる。

(6) 同じオブジェクトをたくさん出現させない

個人情報 DB を入力して計算結果を個人情報 DB に出力するなど、時間の流れに従って記述すると、1 つのオブジェクトをたくさん出現させたくなる。1 組織、1 つフェーズの中にはお同じオブジェクトは 1 つにすることで図をわかりやすくする。それぞれの組織のそれぞれのフェーズで最終的に機密情報がどこにおかれるか、ということを意識して記述する。

(7) なるべく見やすくする配置する

機密情報の流れを示す線はなるべく交差しないように見やすく配置する。ただし、組織を超えて流れる線を途中で切断しまうことはしない。複雑になる部分や組織をまたがる部分にはリスクがあり、それを省略すると、フロー図として意味がなくなる。また、オブジェクトの名前は関与者で共通理解できる業務用語で表現する。10 文字以内で記述することが望ましい。

(8) 最後に流れる情報を見直す

発生から消滅までのオブジェクトをつなげたら、最後に情報の流れを見直します。特に機密情報の流れを強調する、その流れに含まれる特に守秘義務の必要がある情報項目を線やオブジェクトのそばに明記する。その記述によって、誰がどのタイミングで、どんな情報にアクセスし、機密情報がどのように流れていくのかが説明できるようになったら図は完成である。

4. 今後の課題

本報告は各企業での情報セキュリティ対策の実態を調査し、情報セキュリティ対策推進のガバナンス向上の具体策として、「業務データプロセスセキュリティ評価チャート」を提案してきた。すでに、先進企業では本アプローチと同等の見える化を進め始めている。

以下では、今回の実態調査やこれまでの委員会活動で挙げられた「業務データプロセスセキュリティ評価チャート」の課題について、普及活動、標準化活動、制度や法律的な効力の検討、セキュリティ評価技法の観点からまとめる。

4.1. 見える化の普及活動

アンケート調査結果にもあるように、先進企業では「業務データプロセスセキュリティ評価チャート」と同様なフロー図が利用され始めているが、「業務に使った」、「書いたことがある」という回答は少数の企業であった。フロー図を作成することによって、責任分界点を明確にする有効性は感じていても、現場への導入は、その意義や効果が十分理解されておらず、作成に時間かかり、導入が困難であると考えている企業が少なくない。「業務データプロセスセキュリティ評価チャート」の利用を普及させていくには、内部統制、企業グループ統制、業務委託、国際連携など、業務別のひな形の蓄積と作成時間を削減する作図支援ツールの提供が必要であると考える。

(1) ひな形と事例の蓄積

第 3 章のガイドでは具体的な事例として、比較的詳細なフロー図を例として挙げた。初めて作図する場合、もう少し簡略なフローから始め、関与者の示唆により、リスクの高い計算機処理や人的処理を明示化し、関与者との合意形成していくことが重要である。業務へのひな形の蓄積では、必要最低限の処理や作業を記載したひな形を用意し、効果の高い事例を作成して、普及活動を行う事が重要である。

(2) 作図支援ツールの提供

計算機処理・人的処理の矩形の整列やそれをつなぐ情報・業務の流れを示す矢印の結線には作図に慣れた人でも作成時間がかかる。特に、初期作成の後、責任分担を変更する際

にフロー図の変更には手間がかかる。「業務データプロセスセキュリティ評価チャート」の作図を支援するツールの提供を含めた普及活動も重要であると考えられる。

4.2. 見える化の標準化活動(国内、海外)

ヒアリング回答にもあるように、先進企業では委託先との契約での義務付け、オリジナルなフロー図を使っている企業もある。また、印刷業界では業界のガイドとして類似したフロー図が例示され始めている。

(1) 国内での共通化

国内で利用し始めている類似したフロー図の記述形式の長所を取り入れながら、国内での共通化を進め、一定の標準スタイルを作っていくことが重要である。いろいろな記述スタイルが出てくると、複数の企業グループへのサービス提供している中小企業での混乱が起こる。その前に標準的な記述スタイルを定義し普及させることが急務である。

(2) 国際標準への提案

特に海外との連携では、言葉も情報セキュリティに対する意識も異なる。国際連携での普及には国際標準化団体に対しても提案していくことが重要であると考える。

4.3. 制度への導入や法律的な効力の検討

本年度にはプライバシーマーク認定企業が 1 万社、ISMS 認定制度が 3 千社を超えてきている。また、情報システムを用いた事業者にその管理義務を促す法律も整備されてきている。認定制度により蓄積された数多く作業ルールの有効性評価や、法律に対する情報セキュリティの責任分界点や責任分担を計画したことによる管理義務を果たしていることのエビデンスとして効力を検討していくことも必要である。

(1) プライバシーマーク認定制度、ISMS 認定制度

プライバシーマークや ISMS の認定の継続維持には新しい脅威や企業活動（業務）に対する PDCA サイクルによる改善活動が行われる。改善活動によって新しい作業ルールが蓄積されていく。蓄積された数多く作業ルールが当該業務に有効に機能しているかを評価することに利用するなど、既存のセキュリティ対策のプロセスとして導入していくことが期待される。

(2) 法律的な効力の検討

情報セキュリティの責任分界点と責任分担を明確にしたからといって、事件事故が起こ

らないという事ではない。しかしながら、事業者としての最大限の管理義務を果たしているものと考えられる。それらの管理義務を果たすことの効力を明示化していくことも今後の課題である。

4.4. セキュリティ評価技法の開発

保護すべきデータのライフサイクルで起こる計算機処理と人的作業を可視化しても、責任分界点の明確化、セキュリティポイントでの対策の抽出だけでは定性的な議論に終始する。ヒアリング意見にもあるように、それぞれの事象（処理や作業）に対しての発生確率がないと可視化だけで終わる。

(1) 情報漏えいや不正操作の発生確率の基準作り

セキュリティ評価チャートの次のステップとしては、「可視化された事象（処理や作業）に対する情報漏えいや不正操作の発生確率の基準作り」であると考える。発生確率の基準が実装されることによって、どのような情報セキュリティ対策をどこで実施する事が最適な情報セキュリティ対策となるかを定量的に評価できるようになる。しかしながら、FAXやメールでの誤送信の発生確率といっても、手動送信、自動送信、送信先確認、フィルタリングなど、FAX 装置やメーラーの機能によってもその発生確率が大きく変化する。機能を提供するベンダーごとに発生確率の定義が異なっていては共通の基準として利用できない。

(2) 事象の発生確率を用いたセキュリティ対策の最適化技法

個々の事象の発生確率の基準ができたとしても、最終的には全体として事件事故の発生を防止できるかが重要である。個々の事象の発生確率をベースとして機密情報のライフサイクルでの事件事故の発生を最小化し、セキュリティ対策に関わる作業の最適化を計画する技法を開発する必要がある。

参考文献・資料・引用サイト（順不同）

［1］ECOM：EC おけるに個人情報保護に関する活動報告書 2008（平成 21 年 3 月）

［2］JIPDEC ：プライバシーマーク付与事業者一覧（平成 22 年 2 月）
http://privacymark.jp/certification_info/list/clist.html

［3］JIPDEC ：ISMS 認証機関一覧（平成 22 年 2 月）
http://www.isms.jipdec.jp/lst/isr/index.html

［4］JNSA：2008 年 情報セキュリティインシデントに関する調査報告書<改定版 1.3>
（平成 21 年 11 月）

［5］METI：平成 20 年度わが国 IT 利活用に関する調査研究事業（電子商取引に関する調査）報告書（平成 21 年 3 月）

［6］ECOM：EC おけるに情報セキュリティに関する活動報告書 2007（平成 20 年 3 月）

［7］ECOM：EC おけるに情報セキュリティに関する活動報告書 2008（平成 21 年 3 月）

［8］NMDA：「ISMS の維持管理における実態調査」調査報告書（平成 19 年 3 月）

［9］METI、他：個人情報保護ガイドライン改定版（平成 20 年 3 月）

［10］METI、他：：個人情報保護ガイドライン改定版（平成 21 年 11 月）

［11］マイクロソフト：「委託業務の個人情報保護」、
第 35 回 ECOM セミナー講演資料（平成 21 年 2 月）

情報セキュリティ WG(SWG1)メンバーリスト

（敬称略、五十音順）

参加区分	氏　　名	会　社　名
会員メンバー	川嶋　一宏	株式会社日立製作所
	再起　和夫	パナソニック株式会社
	四條信太郎	キヤノン IT ソリューション株式会社
	鈴木　　靖	大日本印刷株式会社 （株式会社 CP コンサルティング）
	行木　直之	マイクロソフト株式会社
	能勢健一朗	東芝ソリューション株式会社
	保倉　　豊	グローバルフレンドシップ株式会社
	吉竹　弘幸	みずほ情報総研株式会社
有識者	荒川　一彦	近畿大学
	岩田　　修	オフィス　イワタ
	垣内　伯之	日本情報処理開発協会
	重松　孝明	有限会社　e－社会研究所
	白川　昭久	株式会社 CP コンサルティング
	高橋　和博	株式会社テプコシステムズ
	辻　　秀一	東海大学
	成瀬　一明	株式会社　東芝
事務局	合原英次郎	次世代電子商取引推進協議会
	山崎　幸男	次世代電子商取引推進協議会

付録 A. アンケート依頼

企業における情報セキュリティ対策の実態と
セキュリティ評価チャートの適用可能性調査票

職場での情報セキュリティ対策の取り組みに関して、該当番号や意見を記入ください。

複数回答可

1. 情報セキュリティ対策の実態について

設問 1-1：2005 年以降の情報セキュリティ対策で得られた効果は？

①情報流出や漏洩の防止・軽減、②情報資産の明確化と整理、③社員意識の浸透と実践、
④事故発生時の体制の整備、⑤セキュリティ事件・事故の減少

回答【　　】その他【　　】

設問 1-2：2005 年以降の情報セキュリティ対策の業務に及ぼした影響は？

①対策コストの増加、②業務量の増加、③手続きの煩雑化・業務効率の低下、
④業務上の制約の増加、⑤対策要員の増加

回答【　　】その他【　　】

設問 1 3：業務量の増加、業務効率の低下、業務上の制約の増加の要因は？

①不要な作業申請等の作成、②不要な作業履歴の記録、③監査目的の資料作成、
④直接業務に無関係な依頼作業の増加、⑤情報を利用・取得しづらくなった

回答【　　】その他【　　】

設問 1-4：情報セキュリティ対策に対する組織幹部の認識

①対策コストが高い、②対策しても利益にならない、③現場のリスクを理解していない、
④事業継続の重要課題と認識している、⑤コンプライアンス(法律)を重視している

回答【　　】その他【　　】

設問 1-5：情報セキュリティ対策に対する従業員の認識は？

①情報セキュリティ意識が低い、②規則を知らない、③形式的な応対が多い、
④自分の業務と合わない規則が多い、⑤無関心・消極的

回答【　　】その他【　　】

設問 1-6：情報セキュリティ対策として必要と思う分野は？

①社内(内部統制)、②業務委託、③企業グループ関係、④国際連携(海外業務委託)
⑤顧客先

回答【　　】その他【　　】

設問 1-7：情報セキュリティ対策として必要と思う基盤は？

①企業内システム、②企業間システム、③クラウド環境、④家庭内 PC

回答【　　】その他【　　】

２．セキュリティ評価チャートの適用可能性

シーン：a.社内、b.業務委託、c.企業グループ、d.国際連携、e.顧客先

設問 2-1：ヒヤリ、ハットした情報管理（受け渡しや情報格納）はあったか？

①頻繁にある、②よくある、③時々ある、④すこしあった、⑤まったくない

回答【　　】シーン：【　　】

設問 2-2：ヒヤリ、ハットした情報の取り扱いのフローは明確となっていたか？

①周知徹底していた、②責任者が知っている、③取り扱いのフローはある、
④不明確だった、⑤意識してなかった

回答【　　】シーン：【　　】

設問 2-3：ヒヤリ、ハットした情報の取り扱いの責任分界点は明確となっていたか？

①関与者間で明確、②部署間で決めている。③管理者に任せている、④不明確、
⑤意識していない

回答【　　】シーン：【　　】

設問：機密情報の取り扱いは関与者の間で責任分担が明確になっていたか。

①関与者間で明確、②部署間で決めている。③責任者だけ決めている、④不明確、
⑤意識していない

回答【　　】シーン：【　　】

設問 2-5：情報取り扱いのセキュリティ評価チャート1を見たことがあるか

①業務に使った、②書いたことがある、③見ている、④類似フローを知っている、

回答【　　】その他【　　】

設問 2-6：企業間利用でセキュリティ評価チャート1の標準化をどう思うか？

①必要、②あれば便利だと思う、③どちらともいえない、④個別に決めるべき、
⑤まったく必要ない

回答【　　】シーン：【　　】

設問 2-7：セキュリティ評価チャート1への意見（ご自由に記入下さい）

：

３．ご回答者様について

①金融、②製造、③流通、④情報システムベンダ、⑤シンクタンク

回答【　　】その他【　　】

①CSO、②CPO、③部門セキュリティ担当、④セキュリティ企画部門、⑤ECOM 会員窓口

回答【　　】その他【　　】

以上

1 次世代電子商取引推進協議会（ECOM）にて共通モデルを検討した機密情報の管理フローを示すモデル

付録 B. アンケート回答

企業における情報セキュリティ対策の実態と
セキュリティ評価チャートの適用可能性調査結果

- アンケート配布先　：ECOM 会員及び個人情報等を取扱う各企業（中小企業等含む）
- アンケート調査期間：3 週間（H21.12.18～H22.1.7）
- アンケート調査数　：150 件
- アンケート回答数　：18 件（H22.1.15 現在）
- 回答要領　　：複数回答可
- 回答の特徴　　：無記入回答有り

1. 情報セキュリティ対策の実態について

設問 1-1：2005 年以降の情報セキュリティ対策で得られた効果は？

①情報流出や漏洩の防止・軽減、②情報資産の明確化と整理、③社員意識の浸透と実践、④事故発生時の体制の整備、⑤セキュリティ事件・事故の減少

回答【①13 件　②12 件　③14 件　④13 件　⑤5 件】その他【なし】

設問 1-2：2005 年以降の情報セキュリティ対策の業務に及ぼした影響は？

①対策コストの増加、②業務量の増加、③手続きの煩雑化・業務効率の低下、④業務上の制約の増加、⑤対策要員の増加

回答【①12 件　②8 件　③8 件　④11 件　⑤3 件】その他【なし】

設問 1-3：業務量の増加、業務効率の低下、業務上の制約の増加の要因は？

①不要な作業申請等の作成､②不要な作業履歴の記録､③監査目的の資料作成、④直接業務に無関係な依頼作業の増加、⑤情報を利用・取得しづらくなった

回答【①3 件　②4 件　③4 件　④6 件　⑤8 件】

意見

1. 社外へ情報を持出す際の申請，履歴の記録(1 件)
2. 上記設問におけるコストは、業務上必要なコストという認識であり、不要なコストと考えていない。(1 件)
3. 影響なし。(1 件)
4. 情報管理に必要な手続き業務の増加(1 件)

設問 1-4：情報セキュリティ対策に対する組織幹部の認識

①対策コストが高い、②対策しても利益にならない、③現場のリスクを理解していない、④事業継続の重要課題と認識している、⑤コンプライアンス(法律)を重視している

回答【①3 件　②3 件　③0 件　④8 件　⑤11 件】

意見

1. 対策のためのコストは必要と考えている。(1 件)

設問 1-5：情報セキュリティ対策に対する従業員の認識は？

①情報セキュリティ意識が低い、②規則を知らない、③形式的な応対が多い、④自分の業務と合わない規則が多い、⑤無関心・消極的

回答【①1 件　②4 件　③5 件　④1 件　⑤1 件】

意見

1. 該当なし(2 件)
2. 従業員の認識は全般的に高くなっている。但し、一部ルールや遵守事項が徹底できていない部分がある(1 件)
3. 情報セキュリティの意識が高い(1 件)
4. 関心は高く、重視しています(1 件)
5. 研修等により必要性を認識しています(1 件)
6. 知識としての理解に止まっているケースをときどき見かける(1 件)
7. セキュリティ対策の通知により認識が高まった(1 件)
8. 一部、①～⑤の該当者がいるが、総じて真摯に取組んでいる(1 件)
9. 当社では情報セキュリティ対策に高い意識を持っている(1 件)

設問 1-6：情報セキュリティ対策として必要と思う分野は？

①社内(内部統制)、②業務委託、③企業グループ関係、④国際連携(海外業務委託)、⑤顧客先

回答【①13 件　②14 件　③7 件　④4 件　⑤4 件】

意見

1. 全て重要と考えますが、特にと言われれば⑤になります(1 件)

設問 1-7：情報セキュリティ対策として必要と思う基盤は？

①企業内システム、②企業間システム、③クラウド環境、④家庭内 PC

回答【①18 件　②6 件　③4 件　④5 件】

設問 1-8：今後の情報セキュリティ対策への意見

回答意見

1. 形式にこだわらず、本来の目的、原点に帰った対策に重点をおけるような施策の実施（例、書式、多少の不備の容認など）
2. マネジメント的対策に加え技術的対策の効果的適用拡大を検討したい
3. 多数の委託先を抱える会社の現状として、目のなかなか行き届かない委託先のセキュリティをいかに確保（担保）するのかが課題

2. セキュリティ評価チャートの適用可能性

（シーン：a.社内、b.業務委託、c.企業グループ、d.国際連携、e.顧客先）

設問 2-1：ヒヤリ、ハットした情報管理（受け渡しや情報格納）はあったか？

①頻繁にある、②よくある、③時々ある、④すこしあった、⑤まったくない

回答【①0 件 ②0 件 ③5 件 ④8 件 ⑤5 件 a.10 件 b.5 件 c.2 件 d.1 件 e.4 件】

設問 2-2：ヒヤリ、ハットした情報の取り扱いのフローは明確となっていたか？

①周知徹底していた、②責任者が知っている、③取り扱いのフローはある、

④不明確だった、⑤意識してなかった

回答【①6 件 ②0 件 ③5 件 ④4 件 ⑤3 件 a.11 件 b.3 件 c.1 件 d.1 件 e.4 件】

意見

1. ルールや遵守事項は明確であったが一部徹底が不十分な部分があった(1 件)

設問 2-3：ヒヤリ、ハットした情報の取り扱いの責任分界点は明確となっていたか？

①関与者間で明確、②部署間で決めている。③管理者に任せている、④不明確、

⑤意識していない

回答【①7 件 ②2 件 ③1 件 ④5 件 ⑤1 件 a.11 件 b.4 件 c.1 件 d.1 件 e.4 件】

意見　設問 2-2 と同じ？

設問 2-4：機密情報の取り扱いは関与者の間で責任分担が明確になっていたか。

①関与者間で明確、②部署間で決めている。③責任者だけ決めている、
④不明確、⑤意識していない

回答【①12 件 ②3 件 ③3 件 ④0 件 ⑤0 件 a.11 件 b.3 件 c.1 件 d.1 件 e.4 件】

意見　設問 2-2 と同じ？

設問 2-5：情報取り扱いのセキュリティ評価チャートを見たことがあるか

①業務に使った､②書いたことがある､③見ている､④類似フローを知っている

回答【①0 件 ②0 件 ③5 件 ④8 件】

意見

1. 見たことがない、知らない(5 件)
2. 当社独自のフローを使用している(1 件 金融機関)

設問 2-6：企業間利用でセキュリティ評価チャートの標準化をどう思うか？

①必要､②あれば便利だと思う、③どちらともいえない、④個別に決めるべき、
⑤まったく必要ない

回答【①0 件 ②10 件 ③5 件 ④3 件 ⑤0 件 a.4 件 b.7 件 c.3 件 d.2 件 e.6 件】

意見

1. 定型的な業務には有効であるが、バリエーションのある業務に関しては有効性は不明である(1 件)

設問 2-7：セキュリティ評価チャートへの意見

1. 低コストで作成できるような、ツールが必要かと思います。
2. 社内でリスク分析を行う際の前工程として類似のチャートを作成しているが、記法の標準化やチャート作成の作業負荷対効果について今後も検討が必要である。
3. あれば便利と思うが、各企業それぞれに独自性があることから、評価チャートについても個別にあるべきと思います。
4. 個人情報は P マーク対応であり、企業機密管理は、社規等の規則や取引先との契約の中で対応している（問題があるとは思っていません)。本件の如き評価チャートの標準化は、ECOM の枠内では機能しないので、不正競争防止法（営業秘密管理指針）や P マーク運用などのスキームを活用する仕掛けがあった方が良いのではないか
5. セキュリティ評価チャートの利用は有効なところもあるが、チャートの作成が業務の

負担増にならないように注意する必要があると感じます。

6. 標準化を進める場合は、各企業の意見を基に十分検討していただきたい。

3. ご回答者様について

(1)業種

①金融、②製造、③流通、④情報システムベンダ、⑤シンクタンク

回答【①2 件 ②2 件 ③1 件 ④8 件 ⑤0 件】

その他

1. 情報サービス提供業
2. 電力(2 件)
3. 非営利団体
4. 製造業
5. 賃貸業

(2) 職種

①CSO、②CPO、③部門セキュリティ担当、④セキュリティ企画部門、
⑤ECOM 会員窓口

回答【①0 件 ②0 件 ③2 件 ④9 件 ⑤5 件】

その他

1. 管理担当取締役
2. 情報システム部門
3. 一般社員
4. SE
5. 内部統制担当

付録 C. ヒアリング内容

「セキュリティ評価チャートのヒアリング」について

経済省受託事業の一環である「セキュリティ評価チャートについてのアンケート」へのご協力、誠に有難うございました。

つきましては、アンケート集計結果を踏まえた上で、業界を代表する主要各社にさらに、下記内容（一部重複）を詳しくヒアリングをすることになりました。

（今回は、各業界としてのお立場からご回答ください。）

1. セキュリティ評価チャートの適用可能性

設問 1-1：

実際に貴社で情報管理（受け渡しや情報格納）をする際に責任分担はどうなっているか？（現場か管理部門か）

（例）①社内データベースにある現場が収集した機密データの情報管理

②社内データベースからダウンロードした機密データ(同上)の情報管理

③モバイルで社外に出たときの機密データ(同上)の情報管理

設問 1-2：

現在、貴社で機密情報の取り扱いの全体フロー図もしくは個別の業務フロー図は作成されているか？

設問 1-3：

万が一、受け渡しの途中に情報漏洩した場合に、情報の取り扱いの責任分界点は明確となっているか？

設問 1-4：

セキュリティ評価チャート は、機密情報の管理（受け渡しや格納）時に、社内の各部門間における責任分界点の検討に役立つと思うか？

設問 1-5：

セキュリティ評価チャート は、情報セキュリティガバナンスの内部統制という観点から有効なツールだと思うか？

設問 1-6：

セキュリティ評価チャート は、企業グループ相互の内部統制という観点から有効なツールだと思うか？

設問 1-7：

セキュリティ評価チャート は、委託業務やアウトソーシングという観点から有効なツールだと思うか？

設問 1-8：

セキュリティ評価チャート は、機密情報の受け渡しを伴う国際取引という観点から有効なツールだと思うか？

2. 本アプローチに対する意見収集

セキュリティ評価チャート（シート）を活用した責任分界点の明確化等の方策について

設問 2-1：

現場でセキュリティ評価チャート(シート)を活用・受入れは実際問題として可能か？

設問 2-2：

困難や不可能な場合、どうしたら活用・受け入れできるか？

設問 2-3：

責任分界点の明確化等の方策としてセキュリティ評価チャート(シート)以外で適切なツールがあるか？

以上

EC の情報セキュリティ推進に不可欠な
項目調査研究活動報告書 2009（SWG2）

平成 22 年 3 月

次世代電子商取引推進協議会 情報セキュリティ WG
（SWG2）

目　次

2. EC の情報セキュリティ推進に不可欠な項目調査研究活動報告(SWG2)----------1
はじめに----------1
2.1. 検疫ネットワーク導入ポイント----------3
2.1.1. 背景----------3
2.1.2. 検疫ネットワークとは----------5
2.1.3. 検疫ネットワークに関する課題認識----------7
2.1.4. 検疫ネットワークの実現----------8
2.1.5. 検疫ネットワークの実現方式----------9
2.1.6. 検疫ネットワーク導入ポイント----------14
2.1.7. 検疫ネットワークの今後----------16
2.2. ハニーポット・マルウェア自動解析
システム･インシデント自動検知システムの利用提言----------18
2.2.1. ハニーポット----------18
2.2.2. ハニーポットの主要なポイント及び注意点----------19
2.2.3. ハニーポットの形態----------20
2.2.4. ハニーポットの運用状況----------21
2.2.5. マルウェア自走解析システム･インシデント自動検知システム----------21
2.2.6. 自動解析システムの代表例----------22
2.2.7. nicter の詳細----------23
2.2.8. ハニーポット・マルウェア自動解析
システム・インシデント自動検知システムの利用提言----------24
2.3. 統合認証基盤構築提言----------25
2.3.1. 各企業における IT の現状及び課題----------25
2.3.2. 統合認証基盤構築に向けての現状----------25
2.3.3. AD 統合を起点とする統合認証基盤の構築例----------26
2.3.4. AD 統合を起点とする統合認証基盤の構築のための代表的なソリューション----------28
2.3.5. 統合認証基盤構築に向けて----------29
2.4.　まとめ----------29
参考文献･資料----------30
情報セキュリティ WG（SWG2）メンバーリスト----------31

2. EC の情報セキュリティ推進に不可欠な項目調査研究活動報告(SWG2)

はじめに

インターネットを介して消費者が事業者から物品やサービスを購入する消費者向けの電子商取引（以下 EC)は、IT 技術の進歩に伴って年々市場規模を拡大している。

EC は、消費者が、端末の代表とされるパソコン（以下 PC）等を利用して、一般的に Web で構成される EC サイトから物品、サービスを購入する際に、端末で動作するブラウザソフトと EC サイトである Web サイトとの間でインターネットを介した通信を行うことで実現する。

EC を成立させるために、消費者は、自らの個人情報（住所、氏名、電話番号、生年月日、性別、カード番号、銀行口座等）を Web サイトに送信する必要があり、Web サイトは、ログインしている消費者が正しく認証されたユーザであることを確認する必要がある。

このような処理を保障する安全・安心な仕組みは、一般的には技術および運用上の仕組みにより可能となる。

しかしながら、近年の Web 技術の急速な進歩に現場のセキュリティ対策が追いついていないことや、ハッカー、クラッカーと呼ばれる攻撃者の攻撃手法が組織犯罪化し、ブラックビジネス化していること等の事情で、Web サイト運営者側の脅威は高まっている。

また、端末側も PC 以外に、携帯電話、スマートフォン、TV 等の情報家電等、様々なものが登場しており、機能向上の反面、利用者操作の複雑さが増して、個人情報売買、なりすまし等の犯罪行為に巻き込まれる等のトラブルも増加している。

近々の国内ネットワークセキュリティの現状傾向をみても、まだまだ P2P ファイル共有ソフトによる情報漏洩事件続発の問題は、依然として解決しておらず、 Winny や Share 利用ノード数も減少せず、暴露ウイルス情報流出による被害が後を絶たない。

さらに、攻撃者の利用する舞台が、Web にシフトしてきており、従来からの SQL インジェクションやクロスサイト・スクリプティングに加えて、DNS キャッシュ・ポイズニングや Hosts ファイルの書き換えや、いわゆる SEO ポイズニングといった新たな攻撃手法が蔓延している。

さらに、2009 年 3 月ごろから広まった Gumblar（日本国内において別名として GENO ウイルスとして呼ばれている）は、Web ページを通じてコンピュータにマルウェアをダウンロードさせ、Web サイトへの改ざん被害を拡大している。

つまり、攻撃する側は、益々巧妙で組織的な活動にシフトしてきている。

これに対する 情報セキュリティ保護の当面の課題及び対策については、即効性のある効果的なものは依然として無く、日頃からの地道な対応（パッチ当てやウイルスチェック等）が基本となる。

しかしながら、従来型のパッシブな（受動的）対策では、パワーアップした攻撃者対策としては不足である。最大のセキュリティホールは人であるという根本真理を前提として、より良いレベルの安全安心な EC 基盤を築くためには、グループ・共同防衛構想ともいうべき情報セキュリティ対策が不可欠であり、能動的（Active）セキュリティシステムの構築が必要となる。

このような状況を鑑み、ECOM EC 安全・安心グループの情報セキュリティ WG のサブワーキング（SWG2）として、複合的（階層的）アクティブセキュリティシステムの構築をテーマにと

りあげた。

本 SWG2 において今年度は、調査・研究活動として位置づけ、検疫ネットワーク導入ガイドラインの作成を目標に、検疫ネットワーク導入ポイントの作成、ハニーポット・マルウェア自動解析システム・インシデント自動検知システムの利用提言及び統合認証基盤の構築提言を行った。

今後、対象と目的を絞ったさらなる調査・研究を行い、複合的（階層的）アクティブセキュリティシステム構築を実現するための共通バイブル（各種ガイドライン等）の策定が重要となる。

2.1. 検疫ネットワーク導入ポイント

ここでは、前述した、複合的（階層的）アクティブセキュリティシステム構築の実現のひとつとして、検疫ネットワークについて記述し、検疫ネットワーク導入のポイントを明らかにするとともに、次年度の検疫ネットワーク導入ガイドライン策定の資とするものである。

2.1.1 背景

ここでは、検疫ネットワークについて、その背景なるものを記述する。

2003 年 8 月に Blaster ワームが出現した。Blaster ワームは、Windows の重大な脆弱性を悪用し、感染を拡大するタイプのワームであった。

発見されたのは 2003 年 8 月 12 日であり、登場してから急速に感染を拡大し、世界中に被害を与えた。Blaster ワームに感染すると、Windows の異常終了や再起動、大量のデータ送信によるネットワーク帯域の消費といった被害が発生し、さらに、ネットワーク内のマシンやインターネット経由で感染を拡大しようとする。

Blaster ワームが流行した理由としては、脆弱性を修正していないパソコンがネットワークに接続しているだけで感染してしまうからであった。Web ページの閲覧や E メールのプレビューすら必要なく、ユーザ側が何もしなくても感染してしまった。

この脆弱性に対する修正パッチは、2003 年 7 月にリリースされていた。Blaster ワームの被害は 2003 年 9 月には沈静化したが、Blaster ワームが残した教訓は大きかった。

Blaster ワームは、ユーザが何らかの行為をしなくても、ネットワークにつないでいるだけで感染し、さらに同じ LAN 内のマシンに感染を拡大しようとするため、特に企業では、外部で感染したモバイルパソコンが社内に持ち込まれ、社内 LAN に接続したとたん、LAN 内に感染が拡大したという例が頻発した。

これは、修正パッチが存在していたにもかかわらず、それを適用していなかったマシンが企業内にあり、それに感染が広がっていったという点で、企業のセキュリティポリシーがしっかりと守られていなかったということである。

同様の被害は、2004 年の Netsky、Sasser といったネットワーク感染型と呼ばれるウイルスでも起こり、いずれも大きな被害を出した。それまで各企業が無策だったというわけではなく、むしろ、様々なセキュリティ製品が導入されていた。

例えば、クライアント側であれば、ウイルス対策ソフト、パーソナルファイアウォールソフト、パーソナル IPS（IntrusionPreventionSystem:侵入防止システム）という製品があり、サーバ側であれば、ゲートウェイ型ウイルス対策製品、ファイアウォール、IPS/IDS（IntrusionDetection System:侵入検知システム）等といった製品である。メールで感染を拡大するタイプのウイルスであれば、ゲートウェイのウイルス対策でブロックできるし、ネットワーク感染型のウイルスもファイアウォールを適切に設定していれば防ぐことができる。IPS/IDS によってウイルス以外の攻撃も防御できる。しかし、Blaster ワーム等は、これらの対策では防ぐことができなかった。

もちろん、本来はクライアント側が適切に脆弱性を解消し、ウイルス対策ソフトやパーソナルファイアウォールソフトを最新の状態にアップデートしていれば、ウイルスの攻撃を防げるはずであった。

セキュリティ意識の高い企業であれば、こうした対策をセキュリティポリシーとして明文化しているところも多い。しかし、Blaster ワーム等の流行によって、これが守られていなかったことが明らかになった。

複数の対策により、LAN 外からの攻撃を防いでいたのに、外から持ち込まれたパソコンによって、内部から感染してしまったのが、Blaster ワームが残した教訓となる。

外からの攻撃を守るだけでなく、内側からの攻撃を未然に防ぐことが重要かつ必要と考えられた。

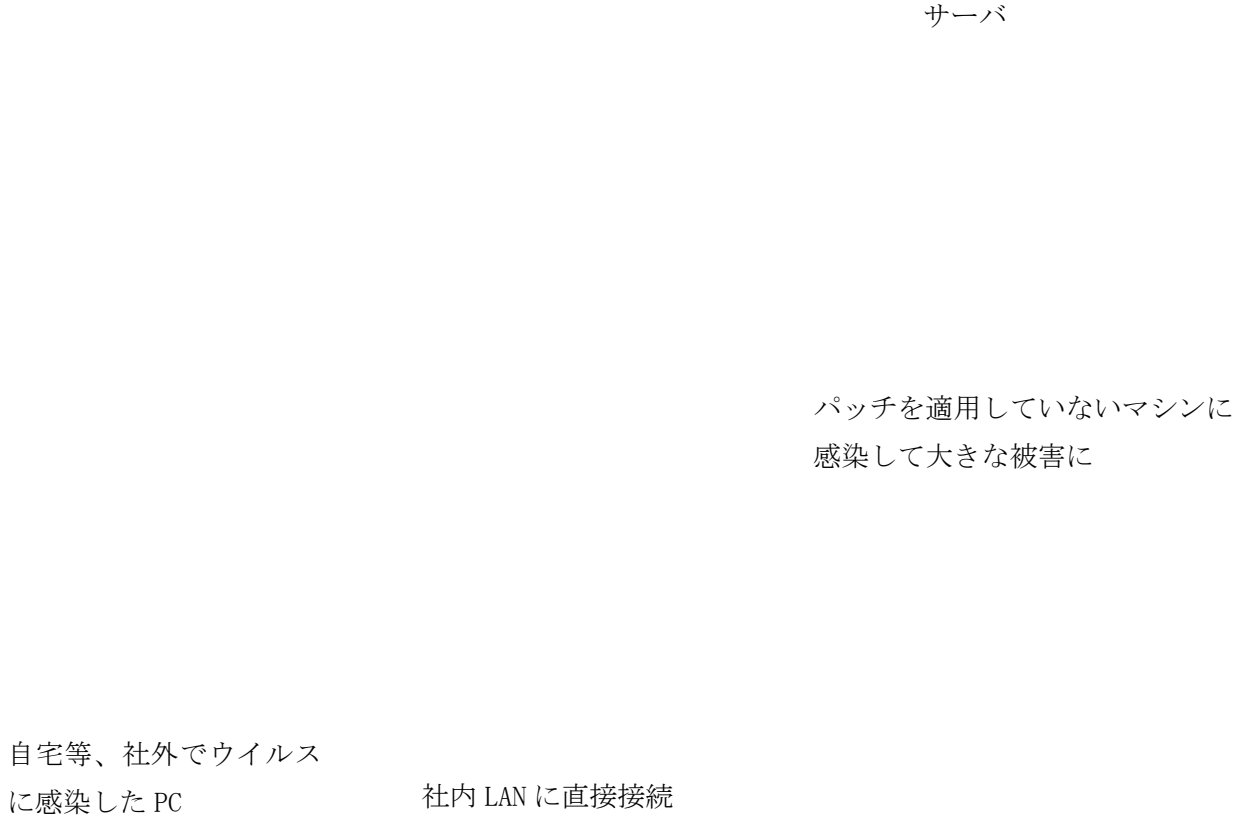


図 1　内側からの攻撃を未然に防ぐことが重要かつ必要

また、2005 年 4 月に個人情報保護法が全面施行された。同法は、一定の数の個人情報を取扱う業者に対して、個人情報を保護するための取組みが義務付けられており、ウイルスに感染して内部から情報が漏えいするといった被害を発生させないことが、ますます重要となった。

情報漏えいやウイルスへの感染等のセキュリティ事故は、内部メンバーの過失（ミス）が原因

となる場合もある。もちろん運用である程度はカバーできるが、セキュリティ事故は、その隙間を縫うように発生する。多くの企業ではノート PC の利用が普及しており、セキュリティ管理者は、これらモバイル端末の管理に頭を悩ませている状況である。

こういったバックグラウンドのもとに、検疫ネットワーク（検疫システムともいう）が考案され、また、注目を浴びることとなった。

2.1.2 検疫ネットワークとは

ここでは、検疫ネットワークとは何かということについて記述し、その目的、必要性等を記述する。

検疫ネットワークは、社内 LAN をウイルス等の被害から守るための決め手として注目されているシステムであり、コンピュータが社内ネットワークを利用する前に、ウイルスへの感染や OS のパッチ適用状況を検査し、問題のないパソコンだけを社内ネットワークにつなぐものである。つまり、検疫ネットワークとは、企業等のネットワークに接続するパソコンを検査する仕組みともいえる。

検疫ネットワークの目的は、ウイルスに感染したマシンを離隔して、他に感染を広げないようにすること、セキュリティポリシーに適合しない危険なマシンを安全なものにすること、安全を確認したパソコンからのみネットワークを利用させることで、社内のセキュリティを確保することである。

一般に、企業内のネットワークとインターネットとの境界にはファイアウォールを導入して、外部からは簡単に侵入できないようになっている。ところが、これだけでは、一度社内に侵入された場合には役に立たない。悪意を持った人が社内に侵入して、自分のパソコンをネットワークに接続すると、サーバにある重要な情報を不正に盗み出されてしまう。ネットワーク上でのやりとりが、いつの間にか盗聴されている危険もある。

問題となるのは社内への侵入だけではない。社員が無自覚のままに、ウイルスやワームに感染したパソコンを持ち込んでしまうこともあり得る。

例えば、会社で使っているパソコンを持ち出して、自宅で作業をしたパソコンをそのまま会社に持ってくることはよくある。こうしたパソコンにウイルスやワームが感染していると、社内のネットワークに接続したときに、一気に感染が広がってしまう。

そこで、パソコンの状態を検査してから、ネットワークに接続させようという仕組みが検疫ネットワークである。社内ネットワークにアクセスしようとするすべてのパソコンは、まずセキュリティの状態を確認するために用意した、特別なネットワーク領域（検査用ネットワーク）に接続させる。検査用ネットワークは社内ネットワーク（社内 LAN）とは切り離されている。

この検査用ネットワークの中で、パソコンの状態が会社の定めたセキュリティポリシーに合っているかどうかをチェックする。

例えば、Windows 等の OS の修正プログラム（パッチ）をきちんと適用しているか、セキュリティ対策ソフトを導入しているか、検出用のパターンファイルは最新版か、問題のあるソフトをインストールしていないかといった内容を確認する。検査に合格したパソコンだけが、接続を切り替えて社内ネットワーク（社内 LAN）を利用できるようになる。

こうしたやり方は、空港等で到着した人や物をチェックする“検疫”と似ている。そのため検疫ネットワークと呼ばれる。空港や港では、目に見えない病気や害虫が持ち込まれるのを防ぐために、入国者の体調に異常はないか、持ち込み禁止とされている物は含まれていないか、動物なら所定のワクチンを接種済みかといった点をチェックする。ここで問題ありと判断された人は、別室で改めて医師の診断を受けるか、持ち込み禁止の物を没収される。検疫ネットワークでも、問題ありと判断されたパソコンは、単に接続を拒否するだけでなく、必要に応じてパッチの適用やセキュリティ対策ソフトの更新といった対策を施して“治療”された後に、改めて検査を受けることもある。

検疫ネットワークを導入すると、社内ネットワーク（社内 LAN）に接続しているパソコンは、必ず一定の条件を満たしているということを保証できるようになる。しかし、それは企業ネットワークのセキュリティのあくまでも一部である。

検疫ネットワークの条件を満たして社内ネットワーク（社内 LAN）に接続したパソコンから、問題となるような操作をされても防ぐことはできない。

例えば、サーバの重要情報や個人情報が漏えいすることを防ぐには、暗号化や文書管理といった、別の対策を併用する必要がある。

ファイアウォール等では外部から持ち込んだノートパソコンによるウイルス等による被害を防ぐことができない、社内 LAN につながる全てのパソコンに対してセキュリティ検査を接続の都度、受けさせることができる、内部メンバーの過失（ミス）を技術的に防ぐことができるといったことが、検疫ネットワークの必要性となる。

図 2　検疫ネットワークの仕組み

2.1.3　検疫ネットワークに関する課題認識

ここでは、検疫ネットワークに関する課題について記述する。

検疫ネットワークはその注目度の高さに比べ、実際の導入がそれほど進んでいないのが現状である。

1 つには、検疫ネットワークを実現する決まった方式がなく、ネットワークの構成やセキュリティポリシーの考え方、導入後の運用方法等を考慮しながら製品を選択する必要があるためだと分析する。

2 つめに、検疫ネットワークが登場した当時と比べて、検疫ネットワークを取り巻く環境が変化してきていることも要因であると考えられる。

検疫ネットワークが登場した当時では、OS やアプリケーションの脆弱性が発見されてから、それを攻撃するウイルスやワーム等の脅威が出現するまでには、しばらくの時間があったため、OS のパッチやウイルス定義ファイルのアップデートが行われていれば、適切に対応ができていた。

例えば、大きな被害を出した Blaster ワームの場合でも、脆弱性が発見されてからワームが出現するまでに約 1 ヵ月かかっており、検疫ネットワークが導入されていれば大規模な感染は防止できたはずである。

しかしながら、現在ではその状況は変わっており、脆弱性が発見されたその日にそれを攻撃する脅威、いわゆるゼロデイ攻撃が現実のものとなっている。OS のパッチやウイルス定義ファイルがリリースされても、すぐにワームの亜種が生み出されるために、最新といわれるパッチやウイルス定義ファイルを適用していても感染する可能性は、おおいにある。

2.1.5 検疫ネットワークの実現方式で細部記述するが、特にクライアント PC に専用ソフトを導入しないタイプの検疫ネットワーク、いわゆるクライアントレスでチェックを行っているシステムの場合、クライアント PC にパーソナルファイアウォール等を導入し、クライアント PC 自身でのセキュリティ対策を施しておかないと感染する恐れがある。

このように、検疫ネットワークだけでは未知の脅威に対応できない場合があるため、別途アノーマリ検出機能を持った IPS 等の導入も併せて検討する必要が出てくる。

最新のパッチやウイルス定義ファイルを適用したくても、社内で利用されているアプリケーションとの動作確認が取れないためにそれらを適用できないといったような運用にかかわる問題もある。このような場合、ポリシーサーバで最新のパッチやウイルス定義ファイルのチェックを行っていると、それらが適用されていないクライアント PC は隔離されてしまう。

このため、ポリシーサーバの定義の更新を遅らせて、特定のクライアント PC に対して例外的にセキュリティ対策状況のチェックを実行しないという運用を強いられ、管理者の負担が大きいものになってしまうということも挙げられる。

検疫ネットワークを含むセキュリティ製品の場合、導入したらそれでおしまいとはいかず、絶えずセキュリティマネジメントサイクルの Plan、Do、Check、Action（PDCA サイクル）に沿った見直しが必要となる。

このようなことから、検疫ネットワークを導入したいと思っていても、上記の理由から導入を見合わせている場合が多いと考えられ、中小企業等を含む各企業が容易に検疫ネットワークシス

テムを導入することのできるガイドラインの作成が課題となる。

2.1.4　検疫ネットワークの実現

ここでは、検疫ネットワークを実現する上での概念を記述する。

検疫ネットワークには厳密な定義がない。そのため，実際に実現する方法は色々とある。例えば、LAN スイッチを使って接続先を振り分ける方法、クライアントにインストールしたパーソナルファイアウォールのポリシーで接続先を切り替える方法、DHCP サーバがパソコンに配布する IP アドレスを変更する方法、ゲートウェイ装置が接続先を振り分ける方法等である。

検疫ネットワークは、様々な実装方法でシステムが製品化されている。基本的には、社内ネットワークと検疫ネットワークを切り替える方法の違いにより、大別して 4 つの方式に分類できる。

いずれの方式でもクライアント PC が満たすべきセキュリティ対策状況を定義した検疫ポリシーサーバを置き、社内ネットワークとは別にセキュリティ対策が不十分なクライアント PC を隔離するための検疫ネットワークを設ける。

図 3　検疫ネットワーク概念図

java、ネットワークテクノロジー、セキュリティ等、最新の IT 技術に関する解説記事 http://www.atmarkit.co.jp を参照

2.1.5　検疫ネットワークの実現方式

2.1.4 で、検疫ネットワークの実現には、基本的に、社内ネットワークと検疫ネットワークを切り替える方法の違いにより、大別して 4 つの方式に分類できると記述した。ここでは、その 4 つの方式について細部記述する。

2.1.5.1　ゲートウェイ方式

ネットワークのセグメントに設置されるゲートウェイで、接続してくる PC を判別する方法である。ルータや VPN 機器等がこれに当てはまる。接続した PC の通信がゲートウェイに達した段階で、検疫済みかどうかを調べ、済んでいれば社内ネットワーク、そうでなければ検疫ネットワークに接続する。

最大の利点は、既存のネットワークに対して大幅な変更が不要な点である。理論的/物理的なネットワーク変更はほとんど必要なく、必要なセグメントごとにゲートウェイを設置するだけで済むため、比較的安価に設置できる。

専用のハードウェアを使うことで、検疫も高速に行える。製品によっては 1 秒程度で検疫が終了するため、クライアント側への負担も少ない。固定 IP や DHCP 環境を問わずに利用できる点も特徴である。

問題点として、セグメントごとに区切られるため、ゲートウェイ内の通信は検疫されない点があげられる。セグメントの区切り方にもよるが、セグメント内に関してはクライアントを接続してワーム感染が広がるといった危険性もある。

一般的にクライアントソフトの導入を行うため、そのコストも必要となるが、クライアントにセキュリティソフトを組み合わせ、セグメント内のセキュリティを確保するソリューションも提供されている。

図 4　ゲートウェイ方式

2.1.5.2 DHCP 方式

DHCP は、IP アドレスを動的に割り当てるためのプロトコルで、企業内では一般的に使われている。この企業内の DHCP サーバを活用し、社内ネットワークと隔離ネットワークに接続する IP アドレスを切り替えることで、検疫ネットワークを実現する仕組みが DHCP 方式である。

この方式を導入した場合、接続しようとするクライアントは IP アドレスを持っていないので、DHCP サーバが IP アドレス付与する。このとき、まず検疫ネットワーク用の IP アドレスをリースし、検疫ネットワークに接続させる。

ここで検疫と治療が行われ、その後正式な社内ネットワーク用の IP アドレスが付与されることになる。

基本的にソフトウェアベースのソリューションであるため、既存のハードウェアやネットワーク構成に変更がいらないので、導入が容易な点が最大の利点である。クライアントソフトも用意されているが、ActiveX を使う等して、ブラウザベースでも検査が行えるので、クライアント側に新たにソフトを導入する必要がない点も利点である。

あらかじめ接続するクライアント PC の MAC アドレスを登録しておくことで、企業が許可していないマシンの接続を拒否する機能もあり、これによって未登録 PC の接続も拒否できる。

ただ、DHCP を利用するため、IP アドレスをクライアントに直接設定していると、検査が素通りされてしまうという、なりすましの問題もある。これについては、IP アドレスを直接設定しているような不正な通信があれば、これを自動検知して通信を妨害するといった対策が必要となる。

図 5　DHCP 方式

2.1.5.3 認証スイッチ方式

IEEE802.1x 認証に対応したスイッチ等を使い、ユーザ認証を行った後に検疫を実施する方式である。VLAN によってネットワークを区別して、検査に通らなかったマシンを離隔ネットワークに接続する仕組みである。

一般的には認証は RADIUS サーバによって行われ、まずユーザ認証を行わなければならない点が特徴である。ユーザ認証をクリアしなければネットワークにアクセスすることはできないため、安全性は高い。ユーザ認証の際、ソリューションによっては、Windows のログオンも同時に行うことができたり、USB トークンを使って認証強度を高めたりといった機能が用意されている場合もある。

スイッチを使うため、ポート単位でアクセス制御が行われ、クライアント別に個別の制御が可能になる。部門によってサーバへのアクセス許可・遮断を設定する等、柔軟な対応が可能である。なお、無線 LAN スイッチ製品で、IEEE802.1x 認証に対応したものも登場している。

ちなみに、IEEE802.1x を使う場合はサプリカントと呼ばれるクライアントソフトが必要となる。WindowsXP には標準でサプリカントが搭載されているが、専用クライアントソフトを要するソリューションもある。ただし、ActiveX を利用して Web ブラウザだけで利用可能にしているサービスもある。

問題点としては、認証スイッチを導入していない場合、機器をリプレースする必要があるといいう点である。クライアントの数に応じたスイッチも導入しなければならず、コスト面に問題がある。

図 6　認証スイッチ方式

2.1.5.4 パーソナルファイアウォール方式

クライアント側に導入したファイアウォールソフトを利用するのがこの方式で、あらかじめソフトを導入しておく必要がある。

パーソナルファイアウォールは、クライアント内外の通信を制御するためのソフトであるが、これを利用し、まず企業ネットワークに接続しようとすると、パーソナルファイアウォールが検疫ネットワークへのアクセスしか許可せず、検疫をパスしたら、そこで初めて制限を解除するというものである。

パーソナルファイアウォール方式では、ネットワーク側の変更が全く不要というのが最大の利点である。モバイル PC を VPN 経由で社内ネットワークに接続させる場合でも、クライアントのパーソナルファイアウォールを使って同様に検査を行うことが可能である。

パーソナルファイアウォールの設定は、集中管理によって管理者が一括して配信できるので、社員が直接設定を行うわずらわしさがない。当然、パーソナルファイアウォールとして、いざというときはウイルスやワームの通信をブロックする働きも備える。

すべてのクライアントにソフトを導入する必要があり、これを導入していないマシンからのアクセスに対して弱い点が問題となる。そのため、一般的には認証 VLAN 装置や VPN 装置等と併用されるソリューションが用意されている。ただ、最近は Web ブラウザを利用することでエージェントソフトの導入を不要とする製品も登場している。

図 7　パーソナルファイアウォール方式

表　検疫ネットワーク実現方式のまとめ

2.1.6　検疫ネットワーク導入ポイント

これまで記述してきたとおり、検疫ネットワークを実現させるためには様々な方式があり、それぞれに利点・欠点がある。これらを加味して、ここでは、検疫ネットワーク導入時のポイントについて記述する。

2.1.6.1 ネットワーク構成の変更及び検疫のための専用機器を必要とするか否か

そもそも組織の LAN はオープンな仕様で構築されているため、LAN を構築するスイッチング HUB や L2/L3 スイッチ、ルータ等のネットワーク機器、また固定 IP、DHCP、IEEE802.1x 等の認証方式を統一していくのは困難である。また、導入が進む無線 LAN 環境への対応も検討せざるを得ない。

これに対し、検疫ネットワークを実現するために専用の検疫ネットワーク用機器を導入するというのも 1 つの選択肢ではある。

ゲートウェイ方式の多くは固定 IP アドレス体系や DHCP 体系、IEEE802.1x 環境のいずれにも適用可能なため、既存のネットワークの設定を大きく変更することがなく、導入が容易であるといえる。

2.1.6.2 専用のクライアントプログラム（エージェントプログラム）が必要か否か

組織には様々なクライアント環境、LAN 環境、ネットワーク環境が存在している。クライアントの OS のバージョンや多岐にわたるウイルス対策ソフトウェア、パーソナルファイアウォール等は主要なものだけでも 10 種類以上は存在し、その組み合わせも多い。

特定のベンダやウイルス対策ソフトウェアに依存しないか、また古い OS をサポートしていない製品や、機能が制限されているケースがないか注意が必要である。また、検疫を実現するためのクライアント端末に特別なソフトウェアやサプリカントソフトウェアをあらかじめインストールすることが必須になるケースがある。このようなエージェントソフトウェアを事前に展開して検疫ネットワークを構築しておくことが必須になることや、パーソナルファイアウォールや関連するポリシーサーバが必要となる等、実現のハードルが高くなる。

製品によっては、Web ブラウザによる端末セキュリティチェックや認証が可能で、クライアント端末に対するエージェントプログラムの導入を必須としないものがある。

2.1.6.3 既存の接続手順との連携、ユーザへの通知と PC の最適化が可能であるか

隔離方式が IEEE802.1x 方式や DHCP 方式の場合、VLAN の切り替えや IP アドレスの更新にまつわるネットワークの接続障害等、管理者が苦労する構成となるケースがあることをある程度覚悟する必要がある。

OS の起動後やログイン後に、ユーザに追加の操作や再度、認証の入力をさせることもある。

理想としては、ユーザには、検疫と接続は意識させないうちに完了しているのが望ましい。

ほぼ全ての製品では、セキュリティ対策に不備のある端末で接続しているユーザや、不正なアカウントで接続を試みるユーザに対しては、検疫の端末セキュリティチェック機能と隔離を行う機器等の認証・ネットワーク制御機能の連携により、検疫エリア以外への接続を拒絶する。

ここからは製品により違いがあるが、セキュリティ対策に不備のある端末に対しては、SUS サーバ等と連携したパッチの自動適用やウイルス対策ソフトの強制起動、ウイルス定義ファイル自動更新作業を強制的に実行させることが可能な製品もある。

これに対し、別途資産管理やインベントリサーバとの連携が必要となる製品があるので注意が必要である。

認証機器の付加機能で実現されているのか、統合化された管理サーバが機能を提供しているのかの違いにより機能性に大きな違いが出てくる。

検疫結果をタスクトレイのアイコンの色の変化やポップアップウィンドウで表示する機能や、検疫が NG の場合には最適化指示や管理者からのお知らせをポップアップさせる機能は管理者、ユーザの双方のユーザビリティを向上させる。

2.1.6.4 既存のユーザ管理との連携、資産管理、インベントリ管理に対応可能であるか

ユーザ/マシン単位で接続許可・拒否を設定することにより端末のセキュリティ状態によらず、接続を許可・拒否することも場合によっては必要となる。

同一組織内であっても開発部隊等、事情がありパッチが適用できない、OS の更新状況が異なる等のユーザ毎の例外条件やグループ毎のポリシーの適用ができることが望ましい。

管理者向けのセキュリティ対策状況の一元管理機能、例えば PC ごとのセキュリティ対策状況一覧、パッチ指定による抽出、セキュリティ不備ユーザへの警告メール送信、リモートデスクトップ接続等の機能も管理者には助かる機能である。これらは資産管理、インベントリ管理機能とともに提供される製品に多く見られる。

2.1.6.5 LAN の拡張や VPN の対応、今後の業界標準への適応が可能であるか

認証スイッチ方式では、主として PC の IP アドレス取得時に検疫を行うため、PC と認証スイッチ間に別の機器が存在している場合や、また、VPN 経由に検疫を実施するということができないということから、LAN の拡張時に適用が容易かどうかは注目すべきである。

ファイアウォール／VPN（IPSec）製品、リモート接続 PC のための SSL-VPN 製品等では、社外から社内へ接続させる際に、検疫が実現できる製品もリリースされている。

こうした PC の社内外の複数のエントリポイントに適用できるような製品が望ましい。ゲートウェイ方式はこうした点で、さまざまな環境で導入が容易なシステムであるいう特徴を持つ。

例えば、検疫ゲートウェイを本社と事業拠点の双方に配置することにより、IPSec VPN トンネル経由や、LAN に接続された PC の検疫のみならず、インターネット VPN 接続された PC の検疫にも対応することができる。

2.1.6.6 検疫サービスの利用

検疫ネットワークを導入したいと思っていても、導入を見合わせているような場合、ISP やキャリアが提供を始めた検疫サービスを利用するのもひとつの手段である。現在はゲートウェイ方式やクライアントファイアウォール方式での提供が中心のようである。

このようなマネージドサービスを利用する場合、検疫ネットワークを導入する側には追加機器やソフトウェアの購入といった新規の設備投資が必要なく、クライアント PC の数に応じた月々の使用料だけで済む。また、日々の運用に関しても、パッチやウイルス定義ファイル情報といったポリシーサーバの定義の更新等もサービス提供者が行うので運用にかかる負担を軽減できる。

まずは、このようなサービスを利用してから、検疫ネットワークを導入し、効果を検証しつつ、今後の検疫ネットワークの標準化等の動きを見ながら、製品選定を行い、検疫ネットワークを展開するのもよい方法である。

2.1.7 検疫ネットワークの今後

最後に、今後の検疫ネットワークの動向について記述する。

検疫ネットワークが注目される中、現状ではベンダに依存した独自規格のシステムが多い中、マルチベンダ環境において、検疫ネットワークを標準化しようとする動きがある。
そのひとつが、Trusted Computing Group（TCG）により発表された Trusted Network Connect（TNC）である。

TCG は、セキュアなコンピューティング環境を実現するためのハードウェアやソフトウェアの業界標準仕様の開発・策定とその推進を目的としており、HP、インテル、IBM、マイクロソフト、サン・マイクロシステムズ等が中心となって設立された業界団体である。

TNC は、マルチベンダのネットワークに接続されるクライアント PC の健全性とセキュリティ状態を判断し、あらかじめ定義されたセキュリティポリシーに基づき、ネットワークへのアクセスを制御するアーキテクチャとして、60 社以上の TCG メンバー企業が参加している TNC のサブグループにより開発されたものである。

TNC の策定にかかわったファンク・ソフトウェアやチェック・ポイント・ソフトウェア・テクノローズ等では、TNC に対応した製品をリリースしている。また、マイクロソフトがリリースした Windows Longhorn Server の検疫機能である NAP（Network Access Protection）も TNC と互換性が保たれている。

TNC を実装するためのふたつの API に「IF-IMC」と「IF-IMV」がある。

「IF-IMC」は TNC クライアントと、パッチやウイルス定義ファイル等のセキュリティ対策状況のチェックを行うクライアント PC が連携するための API である。

「IF-IMV」は TNC サーバとウイルス定義ファイルやパッチを管理するサーバが連携するための API である。

検疫ネットワークの実現方式に、認証スイッチ方式やゲートウェイ方式を採用した場合、例えば、IEEE802.1x 認証を使った認証スイッチ方式の場合、隔離デバイスは L2 スイッチ、TNC ク

ライアントが IEEE802.1x サプリカント（クライアント）、TNC サーバが RADIUS サーバとなる。TNC クライアントは連携しているウイルス定義ファイルやパッチ管理クライアント PC の情報を取得して TNC サーバに送り、TNC サーバは連携しているウイルス対策サーバやパッチ管理サーバにクライアント PC 情報がセキュリティポリシーに適合しているか問い合わせ、その結果に基づいて隔離デバイスに対してネットワークのアクセス制御を行う。

もうひとつの標準化の動きがシスコシステムズの自己防衛型ネットワーク Self-Defensive Network（SDN）戦略に基づく、検疫ネットワークソリューションの Network Admission Control（NAC）である。NAC でも 40 社を超えるパートナーが対応製品をリリース、または対応を表明している。

NAC で利用するネットワーク機器は、シスコシステムズのルータやスイッチで、クライアント PC のウイルス対策ソフトとの連携は、専用クライアントである CTA（Cisco Trust Agent）をインストールすることで実現する。ネットワークへのアクセス制御の仕組みは、TNC とほぼ同じである。

このようにウイルス対策ベンダをはじめ、エンドポイント・セキュリティの多くのベンダが TNC および NAC の両方のアライアンスに参加している。将来的には他のベンダが提唱している方式と標準化がなされ、より良い機能をユーザが選択できるようになると予想されるが、未だ実現されていない。

よって、今後のためにも、より幅広い隔離方式や機器、標準に対応し、検疫ネットワークのみならずエンドポイント・セキュリティの向上や資産管理も含むセキュリティ管理まで拡張可能な製品を導入できるような、ガイドラインの策定に取組んでいくことが重要となってくる。

2.2. ハニーポット・マルウェア自動解析システム・インシデント自動検知システムの利用提言

冒頭で記述したように、より良いレベルの安全安心な EC 基盤を築くためには、グループ・共同防衛構想ともいうべき情報セキュリティ対策が不可欠であり、能動的（Active）セキュリティシステムの構築が必要となる。

このような状況を鑑み、複合的（階層的）アクティブセキュリティシステムの構築のひとつとして、「ハニーポット・マルウェア自動解析システム・インシデント自動検知システムの利用提言」をここに記述する。

2.2.1 ハニーポット

ここでは、ハニーポットについて記述する。

ハニーポットとは、クラッカーの侵入手法やコンピュータウイルスの振る舞い等を調査・研究するために、インターネット上に設置された、わざと侵入しやすいように設定された、サーバやネットワーク機器のことをいう。

「甘い蜜の入ったつぼ」の意味で、クラッカーやウイルスを「おびき寄せる」という意味からこのように呼ばれる。

ハニーポットは、ネットワーク越しには単なる脆弱なサーバやネットワーク機器にしか見えないが、侵入しても外部に攻撃できないような設定がされており、また、侵入者やウイルス等が介入できない方法で詳細な記録を採っている。

これは、ハニーポットにおびき寄せられた侵入者の行動記録を調査することによって、コンピュータへの侵入や攻撃の手法を研究して、いち早くウイルスの亜種を「捕獲」して分析するといったことである。

セキュリティ対策ソフト等は、日々新しく考案される侵入手法に迅速に対処する必要があるため、ハニーポットから得られる情報は有効な対策を考える上で非常に有用な情報となり得る。

また、重要なサーバとは別に、ハニーポットを設置しておくと、攻撃者の興味は脆弱なハニーポットへ向けられるため、重要なサーバへの攻撃をそらし、攻撃者の行動を把握することもできる。

しかし、ハニーポットで収集されるデータは多岐にわたり、そのデータをもとに、攻撃の手法や不正な行為の証拠を特定するには、多くの知識や経験と時間を必要とする。

また、ハニーポットは「本当に」侵入されてはならない。つまり、ハニーポットを動作させている基盤のシステムを乗っ取られたり、ハニーポットを踏み台に他のネットワークを攻撃されたり、不正なファイル交換に利用されてはならない。よって、侵入を許しつつ、実際の被害を抑えるようなシステムを設置・運用しなければならないものであり、非常に高度な知識と技術を要する。

図 8　ハニーポットの仕組み

2.2.2 ハニーポットの主要なポイント及び注意点

ここでは、前述で説明したハニーポットの主要となるポイントを下記に記す。

●見かけも動作も本物そっくりにする。

●攻撃者等に飽きられないよう、適度な内容更新を行う。

●ハニーポット自身の存在が明らかにならないようにする。

例えば、監視やログの収集は、ハニーポットのコンピュータとは別にして、こちらは外部からの操作を一切受け付けない（攻撃者等からはコンピュータが停止しているように見えるのが望ましい）ように設定しておく。

●ハニーポットが危うくなったときのために、回線を遮断する機能を備える。

●非武装地帯（DMZ）に設置する。

●侵入を検知したら、すべての侵入者の行動記録をとる。

●ハニーポットの運用にあたっては、ファイアウォール等基本的なセキュリティ対策を講じておく。

●侵入を検知したときの対処について、体制とフローを確立しておく。

また、ハニーポットの主要となるポイントと裏腹の関係になる、ハニーポットの注意点について下記に記す。

●ハニーポットで収集したデータをもとに、攻撃の手法や不正な行為の証拠を特定するには、多くの知識や経験と時間を必要とする。

●「本当に」侵入されてはならない。つまり、ハニーポットを動作させている基盤のシステムを乗っ取られたり、ハニーポットを踏み台に他のネットワークを攻撃されたりされてはならない。侵入を許しつつ、実際の被害を抑えるようなシステムを設置・運用することが要求される。

2.2.3 ハニーポットの形態

ここでは、ハニーポットの形態について記述する。

ハニーポットは、目的に応じて設計されるので、目的の数だけハニーポットの形態があるといえるが、実現方法によって、次のように分けることができる。

●高対話型ハニーポット

The Honeynet Project のハニーネットのように、実際に脆弱性を残した「本物」の OS やアプリケーション等をハニーポットとして利用する。

「本物」を使用するため、高度な情報を得ることができるが、侵入されたときのリスクが高い。また、ハイ・インタラクション型ハニーポットと呼ばれることもある。

●低対話型ハニーポット

特定の OS やアプリケーションをエミュレートし、監視を行うものである。エミュレートした範囲に機能が制限されるので、高対話型に比べ比較的安全に運用ができる。ただ、機能を限定しているので情報量は落ちてしまう。

特定用途向けのハニーポットであり、Honeyd、Spector、GHH ("Google Hack" Honeypot)、mwcollect 等がある。また、ロー・インタラクション型ハニーポットと呼ばれることもある。

●仮想ハニーポット

仮想機械（VMware や Xen 等）で構成されたハニーポットである。仮想機械を用いることで、ホストを侵入前の状態に戻したり等、リスクを抑えたり、管理面で有効な方法である。だが、ボットの種類によっては、仮想機械であるか調べるものがあり、仮想機械の特徴を調べることで、ハニーポットで監視していることが侵入者に知られる可能性がある。

●分散型ハニーポット

集中管理するハニーネット（ハニーポットが 1 台のおとり用コンピュータを用意するのに対して、ハニーネットは複数のコンピュータで成り立っているおとり用ネットワークを用意する。仮想コンピュータと仮想ネットワークを使い 1 台のコンピュータ上にハニーネットを構成する事ができる。）とは異なり、遠隔地のハニーポットのデータを集中的に管理分析する。

●ハニーポットファーム

GRE（General Routing Encapsulation）等で転送された通信を管理されたハニーポットで集め監視するものである。ハニーネットの様にハニーポット用に管理されたネットワークを用いて、遠隔地の監視を行う。侵入に伴うリスクを集中することができ、複数個所（物理的に遠隔地）にハニーポットを設置することをしないで監視が可能となる。しかし、転送に伴う遅延時間が避けられないため、転送による遅延時間により、侵入者にハニーポットファームであることを知られる可能性がある。

2.2.4 ハニーポットの運用状況

ここでは、ここまで記述してきたハニーポットの運用状況について記述する。

ハニーポットは、EC サイト等の重要なサーバと併設して不正アクセスを早期検知し、犯罪の証拠保全用、大学やセキュリティベンダーが攻撃者の手口を調査・研究する等の目的で設置・運用されている。

商用製品としてもSymantecのDecoyServerやスイスNetwork Security社のSpector がある。

ハニーポットに関する研究プロジェクトとしては、ハニーネット・プロジェクト（The Honeynet Project）が有名である。

ハニーネット・プロジェクトは、コンピュータセキュリティ、情報の収集分析、情報心理学の専門家で構成されるグループであり、ハニーネットを開発、実行している。

ハニーネット・プロジェクトが設置したハニーポットは、侵入者たちがうろつくのに十分なほど広い。あちらこちらに障害物が置かれ、どれも熱中できる程度には難しいが，嫌になってあきらめてしまうほどではないレベルに仕組まれている。

ハニーネット・プロジェクトが設置したハニーポットへの最初の攻撃は 2000 年 6 月 4 日であり、設置されて 1 週間とたたないうちに侵入されたようである。

その後の観察結果によると、攻撃者等の多くは、情報にアクセスしたいからシステムに侵入するのではなく、単に侵入できるから進入すると分析されている。

2.2.5 マルウェア自動解析システム・インシデント自動検知システム

ここでは、マルウェアとインシデントの現状及びその関係について記述する。

近年、マルウェアの攻撃力は日々増大しており、最近発生したインシデントの背景には、必ずマルウェアが存在する状況にある。

米セキュリティ企業の McAfee は、2009 年上半期のマルウェアの動向についてまとめたホワイトペーパーを発表し、半年間で見つかったマルウェアの数が 2008 年の 1 年間に検出された数に迫るレベルになったと報告した。

McAfee によると、マルウェアの検出数は 2008 年にそれまでの年と比べて突出した伸びを示したが、2009 年はそれをさらに上回る勢いで増え、上半期だけで比べると 2008 年の 3 倍に増加した。

平均すると月間 20 万種類、1 日に 6000 種類のマルウェアが検出されている計算になる。

マルウェアはユーザをだましたり、個人情報を盗んだりする目的で使われており、犯罪者が金儲けをするためのビジネスとして成立するようになった今、不況の中でも勢力が衰える気配はない。マルウェアのコードや作成ツールも簡単に手に入るようになっている。

こうした状況は当面改善されそうにないと McAfee は述べており、ユーザの啓発とソフトウェアやウイルス定義ファイルを常に最新の状態に保つことが役に立つと解説している。

一方、JPCERT/CC は、インシデント・ハンドリングを主な活動とする非営利組織である。日本国内の Web サイトで発生したセキュリティ・インシデントの報告を受け付ける窓口となり、攻撃手口の分析や、対策の検討および助言を行っている。

また、「寄せられたインシデント情報が二次的に悪用されないように、情報を管理する役目を担っている。」

2009 年 4 月～6 月に JPCERT/CC に報告されたインシデントの内訳は、コンピュータに不正侵入する「マルウェア」が 43%、攻撃を目的にパソコンや Web サイトの弱点を検索する「スキャン系」が 20%、情報を盗む「フィッシング」が 15%、Web サイトへの「侵入／改ざん」が 5%、「その他」が 17%であった。

この傾向について、スキャン系、フィッシング、Web 改ざんといった攻撃にもマルウェアが関わっていると分析される。よって、インシデントの背景には必ずといっていいほど、マルウェアが存在するという認識とした。

インシデントの背景に存在するマルウェアの特徴は、実用性を意識して作られていることである。パソコンに感染したマルウェアは、ハードウェアに負担をかけずに静かに活動し、パソコンのパフォーマンスを監視しても、感染に気がつかないほどである。また、作成ツールが高度化し専門技術がない人でも GUI で簡単に複雑なマルウェアを作成できるため、最近のマルウェアは単純なパターニングだけでは検知できないほど複雑化している。

こうした進歩により、マルウェアに感染してボット化したパソコンは、もはや攻撃インフラであり、ひとつのウイルスの何倍もの攻撃力を持つ。

さらに、簡単にカスタム・マルウエアが作成できるようになったため、マルウェアを使った標的型攻撃も増加傾向にある。スピア（標的）型攻撃においては、不正な細工を施したメールを開封させるために、時事ネタや個人情報を巧みに使って信用させる、ソーシャルエンジニアリング的手法が発達してきた。

このようなマルウェア攻撃を防御するには、アセンブラコードを追う地道な解析も必要だが、マルウェアを自動的に解析するマルウェア自動解析システムの構築と解析したマルウェアの最新情報を防御側で利用する等といった、連携が重要になってくる。

2.2.6 自動解析システムの代表例

ここでは、前述であったとおり、インシデントの背景には必ずといっていいほど、マルウェアが存在するということから、情報通信研究機構（NICT）が開発した、マルウェア自動解析システムを代表例として記述する。

情報通信研究機構（NICT）は、サイバー攻撃等の検出・分析・対策等を容易に行えるネットワークを実現するための技術や、情報・プライバシー保護のための暗号・認証技術等の研究開発を行っている。

情報通信研究機構（NICT）は、ネットワーク上の攻撃を検知し、自動解析、相関分析を行うセキュリティ・インシデント分析システム「nicter（Network Incident analysis Center for Tactical Emergency Response）」を開発した。

nicter は、ネットワーク上で観測、検知した攻撃をマクロ、ミクロの両方の視点から自動分析し、可視化するシステムである。

サイバー攻撃の増加、多様化により、従来からの半手動型の解析が困難になってきていることを踏まえ、セキュリティログをもとに、攻撃を自動的に分析して、高い精度でマルウェアを自動

解析する技術を実現するものである。

Nicter のシステムは、広域ネットワークを観測し、攻撃をリアルタイムに自動分析するマクロ解析システム、ハニーポット等によってマルウェアを捕捉し、検体 1 つを 5 分程度で自動解析するミクロ解析システム、解析結果の相関を調べ、ネットワーク上で起こっている現象とその原因を結び付けるマクロ-ミクロ相関分析システム、一連の分析結果を集約、管理し、可視化して表示するインシデントハンドリングシステムからなる。

Nicter の情報源を以下に記述する。

●ISP からの実トラヒック

●実ホストの存在しない未使用アドレス（群）　10 万以上の IP アドレスを観測

⇒400～600 MB/day を観測する。

●国内大学ネットワークに設置された IDS のログ

⇒100 MB/day を観測する。

●ハニーポット・ダミーメールアカウント・Web クローラ

⇒攻撃コード、マルウェアの検体を取得する。

⇒メール添付型ウイルスを収集する。

⇒Web クローラでメールアーカイブを取得し、メール添付型ウイルスを収集する。

2.2.7 nicter の詳細

ここでは、nicter の詳細として、システムごとについて記述する。

2.2.7.1 マクロ解析システム

マクロ解析システムは、振舞分析（Traffic Analysis ＆ Profiling）と呼ばれる分析を行う。振舞い分析は、攻撃ホスト（送信元 IP アドレス）ごとに、短時間（30 秒）の挙動を分析し、スキャンの振舞を「送信元ポート番号」、「宛先 IP アドレス/ポート番号」、「プロトコル種別」、「シーケンシャル/ランダムスキャン」によって自動分類し、データベース化する。

また、新規の攻撃パターンを自動検出し、変化点検出（Change Point Detector）として、 観測トラヒックの急激な変化を自動検出する。

2.2.7.2 ミクロ解析システム

ミクロ解析システムは、静的解析（Malware Code Analyzer）と呼ばれるホワイトボックスアプローチ及び動的解析（Malware Behavior Analyzer）と呼ばれるブラックボックスアプローチを行う。

静的解析は、難読化されたマルウェアのコードを解析するため、メモリ上に展開された、マルウェアをダンプし、解析する。

動的解析は、仮想的なインターネット環境の中でマルウェアを動作させ、その挙動を抽出するものである。

2.2.7.3 マクロ-ミクロ相関分析システム

マクロ-ミクロ相関分析システムは、マクロ解析による、新規の攻撃パターンとミクロ解析によるマルウェアの解析結果を突合せて、相関性を調べ、現象と原因を関連付けるものである。

また、当該ホストが感染している可能性の高いマルウェアの候補リストを出力する。

2.2.8 ハニーポット・マルウェア自動解析システム・インシデント自動検知システムの利用提言

ハニーポットにおいては、ハニーネット・プロジェクトの活動、マルウェア自動解析システム・インシデント自動検知システムにおいては、情報通信研究機構（NICT）が主体となって開発した nicter を主体に記述してきた。

マルウェア等を解析するための情報源のひとつとなるハニーポットや nicter は、より良いレベルの安全安心な EC 基盤を築く、複合的（階層的）アクティブセキュリティシステムの構築を実現するひとつとして重要なものである。

ここで、ECOM EC 安全・安心グループの情報セキュリティ WG のサブワーキング（SWG2）としては、研究機関等の研究を研究のための研究に終わらせることなく、研究効果を商用におけるセキュリティ対策に反映することを要望したい。

今後、安全安心な EC 普及のためにも、研究機関等で得た情報等と民間セキュリティサービス業との連携を図った、組織的な、ウイルス等の捕獲・駆除等のシステムの実現をここに提言する。

2.3 統合認証基盤構築提言

2.1 で記述した検疫ネットワークに関する事項、2.2 で記述したハニーポット・マルウェア自動解析システム・インシデント自動検知システムの利用提言に引続き、複合的（階層的）アクティブセキュリティシステムの構築を実現するひとつとして、統合認証基盤の構築ついて提言する。

2.3.1 各企業におけるITの現状及び課題

ここでは、各企業における IT の現状について記述する。

各企業においては、業務に深く関わるシステムが部門ごとに多数存在し、多種多様なアプリケーションが動作している。これにより、アプリケーションごとに ID とパスワードがばらばらであり、その上、何度もログインが必要なため、結局、付箋等に書いて、PC に貼ったりする等の利用者が多くなる。

さらに、アプリケーションごとにいくつもの本人認証機能（例えば、指紋認証や IC カード認証）を採用しているのも現状である。

また、管理者側からすると、セキュリティポリシーやアクセス権がアプリケーションごとにばらばらに管理されていて、運用するのが大変であり、認証や利用状況のログがアプリケーションごとに分散していることにより、集約して全体を把握することが難しいといえる。

情報漏洩防止や不正行為を IT システム上で防止するためには、セキュリティの強化やセキュリティポリシーをもとに、一貫して管理されたセキュリティシステムの構築が重要であり、統合認証基盤の構築が課題となる。

2.3.2 統合認証基盤構築に向けての現状

ここでは､統合認証基盤の構築を課題と認識し､統合認証基盤構築に向けての現状を記述する。

WindowsNT や Windows2000 を基盤としたネットワーク時代においては、論理的に 1 グループとして扱う、NT ドメインを中心としたシステム運用がされていた。

NT ドメインのユーザ管理データベースには、4 万人程度までのキャパシティであり、大規模なユーザ収容が困難であった。

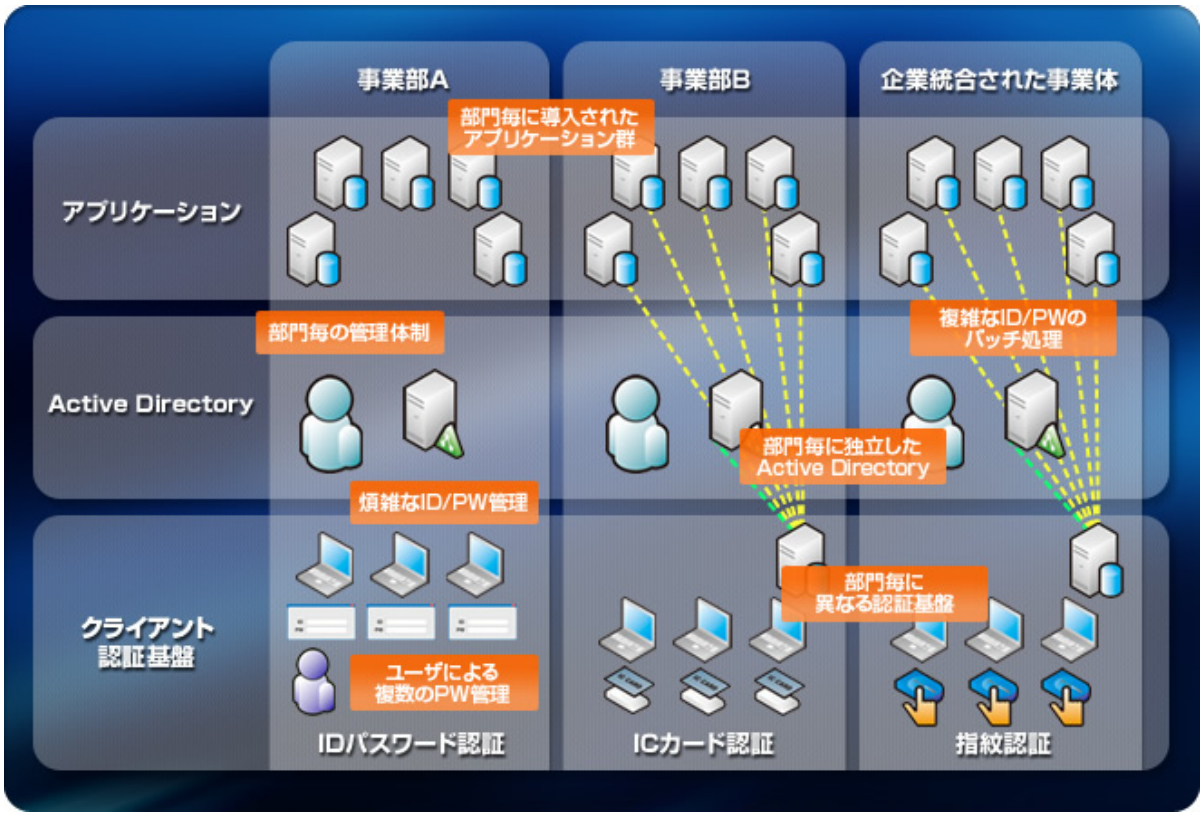
また、複数の大規模拠点を繋ぎ、NT ドメインの統合環境を構築した場合、回線を圧迫していた。こういった制約から、NT ドメイン時代は拠点や部門ごとの分散管理傾向にあった。

このような、分散管理の構成を見直すことなく、Active Directory（以下、AD）を導入し、AD の乱立状態となった。

その後、AD を 1 つに再構築する動きとなったが、多数のアプリケーションによる、多数の ID 及びパスワード分散問題、本人認証の乱立（ID パスワード認証、指紋認証、IC カード認証等）については、未だ解決に至っていない現状である。

最近、注目されてきている、ユーザが一度認証を受けるだけで、許可されているすべての機能を利用できるようになるシステム Single Sign-On（以下、SSO）は、ID・パスワードを見かけ上統合するものであり、上記の根本的解決策とはなっていない。

よって、AD を中心に IT 基盤の確立を目指す多くの企業は、実際には理想とほど遠い現実に置かれている。



https://www.netsecurity.ne.jp より引用

図9　統合認証基盤構築に向けての現状イメージ

2.3.3　AD 統合を起点とする統合認証基盤の構築例

ここでは、AD 統合を起点とする統合認証基盤の構築例を記述する。

● AD 統合をベースとした認証基盤の統合

AD を再構築して統合し、PC やユーザの一元管理と統合的なセキュリティ管理を行い、Windows 統合認証基盤の基礎とするものである。

AD 統合のメリットを以下に記述する。

- 部門をまたがる業務フローの構築が容易になる。
- セキュリティポリシーの整合性が確保できる。
- 部門をまたがる移動なのでユーザ情報管理を容易にする。

● AD やアプリケーション群の ID 管理環境の統合

AD やアプリケーション等の ID を統合することで、全てのシステムに対して同じユーザのアカウントを一意にし、統一された ID・パスワードで全てのアプリケーションを利用するものである。

ID 統合のメリットを以下に記述する。

- ID とパスワードの管理コストを削減し、メンテナンス性についても飛躍的に向上でき

る。

・　ユーザが複数のパスワードを管理することで、発生するセキュリティの低下を防止することができる。

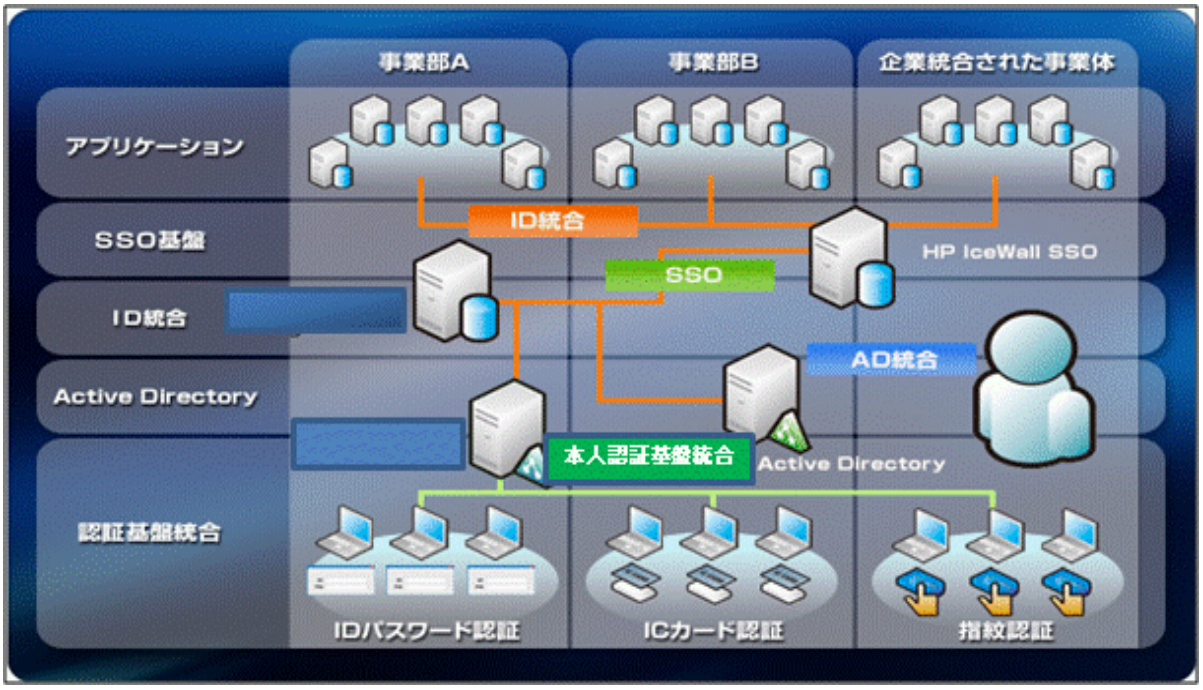
・　人事異動等による ID 管理が確実に行える。

● 電子証明書の管理機能

電子証明書の発行・更新・失効等の管理を一元的に行うものである。

● 本人認証基盤の統合

AD と連携した本人認証及び多要素認証（ID パスワード認証、指紋認証、IC カード認証等）環境を構築するものである。



https://www.netsecurity.ne.jp より引用

図 10　AD 統合を起点とする統合認証基盤イメージ

● SSO の構築

Windows 統合認証を利用できない場合、SSO の導入検討が必要となる。

2.3.4　AD 統合を起点とする統合認証基盤構築のための代表的なソリューション

ここでは、AD 統合を起点とする統合認証基盤構築の一例として、代表的なソリューション等について記述する。

2.3.4.1 Microsoft Identity Lifecycle Manager 2007(以下、ILM 2007)

ILM2007 は、異なる ID 管理環境を統合するとともに、電子証明書の管理についても一元的に行うものである。つまり、AD と連携した統合認証基盤の構築を実現するものであり、主要な機能を以下に記述する。

- ID 統合（ディレクトリ同期）
- パスワード管理
- 電子証明書・スマートカード管理

2.3.4.2 EVE MA

EVE MA は、AD の環境を生かしながら、多要素認証（ID パスワード認証、指紋認証、IC カード認証等）を組み合わせるソフトウェア製品である。

つまり、IC カード認証や生体認証等、ベンダを問わず、様々な認証システムを導入できるフロントエンドの役目を果たすものである。

2.3.4.3 HP IceWall SSO

HP IceWall SSO は、数百万ユーザとなる大規模ユーザ環境でも、快適な環境が実現できるパフォーマンスとスケーラビリティをもつものである。

また、多彩な認証方式に対応し、AD 統合をベースに EVE MA で構築した基盤の中に組み込むことができる。

さらに、エージェントレスで OS や Web アプリケーションに制限の少ないリバースプロキシ方式を主体とした Web シングルサインオン製品である。

2.3.4.4 OpenLDAP

最初の LDAP の実装であった米ミシガン大学の SLAPD（stand-alone LDAP daemon）はインターネット上で公開され、拡張が続けられてきたが、事実上その開発はオープンソースの OpenLDAP に引き継がれている。OpenLDAP はソースコードを公開しているオープンソースのソフトウェア（無償）で，Linux や FreeBSD などのオペレーティングシステム上で広く使用されているものである。

2.3.5 統合認証基盤構築に向けて

統合認証基盤の構築に向けて､情報漏洩防止や不正行為を IT システム上で防止するためには、セキュリティの強化やセキュリティポリシーをもとに、一貫して管理されたセキュリティシステムの構築が重要であるということから、統合認証基盤の構築を課題とし、多数のアプリケーションによる､多数の ID 及びパスワード分散問題､本人認証の乱立（ID パスワード認証､指紋認証､IC カード認証等）問題を解決するために､AD 統合を起点とする統合認証基盤の構築例を記述し、それを実現するための代表的なソリューションを記述してきた。

統合認証基盤は、複合的（階層的）アクティブセキュリティシステムの構築を実現するひとつの基盤として重要であるため、今後、統合認証基盤構築に向けての技術的ガイドラインの策定に取組んでいくことが重要になってくる。

2.4 まとめ

検疫ネットワークシステムにおいては、導入ポイントまでを記述し、今後、さらなる調査・研究を積み重ね、検疫ネットワーク導入ガイドラインの策定に取組みたいと考える。

ハニーポット・マルウェア自動解析システム・インシデント自動検知システムの利用提言、統合認証基盤の構築に関しては、その実現を見守るほか、類似するサービスの利用等について、調査・研究に取組みたいと考える。

さらに、これらの調査・研究を包括的にとらえ、今後、対象と目的を絞った、包括的な調査・研究を行い、複合的（階層的）アクティブセキュリティシステムの構築を実現するための共通バイブル（各種ガイドライン等）の策定を目標として行きたい。

参考文献・資料・引用サイト(順不同)

1　日経 BP 社が運営する、IT（情報技術）にかかわる総合情報サイト
http://itpro.nikkeibp.co.jp

2　java、ネットワークテクノロジー、セキュリティ等、最新の IT 技術に関する解説記事
http://www.atmarkit.co.jp

3　最新のソリューションやサービス、製品動向などの実務情報サイト
http://www.bcm.co.jp

4　企業向け IT 製品サイト
http://www.keyman.or.jp

5　検疫ネットワークを実現する仕組み　　著者：小山安博

6　検疫ネットワークが必要とされるワケ　著者：小山安博

7　IT 製品比較サイト
http://japan.zdnet.com

8　テクノロジー関連のニュース及び速報を中心とした、レビューや特集記事の掲載サイト
http://www.itmedia.co.jp

9　JPCERT/CC サイト
http://www.jpcert.or.jp

10　The Honeynet Project サイト
http://project.honeynet.org

11　内閣官房情報セキュリティセンターサイト
http://www.nisc.go.jp

12　セキュリティ及びネットビジネスに特化した、調査レポート等の掲載サイト
https://www.netsecurity.ne.jp

情報セキュリティ WG(SWG2)メンバーリスト

（敬称略、五十音順）

参加区分	氏　　名	会　社　名
会員メンバー	川嶋　一宏	株式会社日立製作所
	再起　和夫	パナソニック株式会社
	四條信太郎	キヤノン IT ソリューション株式会社
	鈴木　　靖	大日本印刷株式会社 （株式会社 CP コンサルティング）
	行木　直之	マイクロソフト株式会社
	能勢健一朗	東芝ソリューション株式会社
	保倉　　豊	グローバルフレンドシップ株式会社
	吉竹　弘幸	みずほ情報総研株式会社
有識者	荒川　一彦	近畿大学
	岩田　　修	オフィス　イワタ
	垣内　伯之	日本情報処理開発協会
	重松　孝明	有限会社　e－社会研究所
	白川　昭久	株式会社 CP コンサルティング
	高橋　和博	株式会社テプコシステムズ
	辻　　秀一	東海大学
	成瀬　一明	株式会社　東芝
事務局	合原英次郎	次世代電子商取引推進協議会
	山崎　幸男	次世代電子商取引推進協議会

秘密分散技術利活用検討における
活動成果報告書 2009（TF1）

平成 22 年 3 月

次世代電子商取引推進協議会 情報セキュリティ WG
タスクフォース 1

目 次

1. はじめに 1
2. デジタルデータの特性 2
3. 情報セキュリティ技術の原点と秘密分散技術 3
4. 秘密分散技術の安全性と技術要件のあり方 5
5. 秘密分散技術に関する利活用のあり方 7
6. ガイドラインについて 9
7. 法的提言 9
8. 終わりに 9

1. はじめに

昨今の情報社会における大きな問題は、一般にセキュリティレベルが高いと考えられていた企業・組織から、保護・管理対象となっている情報が、続々と漏洩していることである。これは、情報システムを社会基盤としてとらえ国家戦略を推進している我が国にとって、早急に解決策を具体化しなければならないという事実を我々に突きつけているものと言えよう。

このような状況の下、経済産業省が公開している個人情報保護法のガイドラインや、内閣官房情報セキュリティセンターが公開している統一基準解説書で、情報セキュリティ担保のための新たな情報保護技術・措置として暗号以外の技術も散見されるようになってきた。その中の 1 つに秘密分散技術があるが、本技術は情報セキュリティの観点で非常に有効な技術であるものの、暗号技術ほど世の中に認知されているものとはいい難い状況である。そこで次世代電子商取引推進協議会では、2009 年度情報セキュリティ WG 配下において秘密分散技術利活用検討タスクフォースを実施し、秘密分散技術の利活用方法について一定の見解を示すこととした。本報告書はその活動成果報告を行うものである。

なお、秘密分散技術を少しでも利活用しやすい形とするため、本報告とガイドライン、法的提言の 3 部構成とさせていただいた。別紙となるガイドラインおよび法的提言についても目を通されたい。

2. デジタルデータの特性

我々が会社や自宅で利用しているパソコンや、オーディオ機器、その他デジタル技術が適用されている仕組みでは、利用する情報を 0 と 1(この 0 や 1 をビットと呼ぶ)で構成されるデジタルデータとして扱っている。例えば、「あ」とワープロで入力した際に、実際にコンピュータが扱っているデジタルデータは、「1000001010100000」と、0 と 1 が 16 ビット分利用されて記録される。数字で、「20」を入力すれば、「0011001000110000」である。このように 0 と 1 の並びで情報を表示・表現(情報自体の意味)を記録し扱うのがデジタルデータの世界である。

この時、例えば、「あ」＝「1000001010100000」に対し「1000001010100010」と、最後から二番目の「0」を「1」に変えてしまうと、「あ」の表現・情報の意味は無くなってしまう。この状態は、「原本性が損なわれた状態」であり、誰かが故意にいたずらや嫌がらせ等で行うと、世間一般で言う「改竄」という事態となる。

更に、「あ」＝「1000001010100000」のデジタルデータ(原本情報)の 0 と 1 のビットの並びのうち、最初の「1」が無くなったら(000001010100000)、どのようなことになるのだろうか?

コンピュータの世界では、一定のルールによって「あ」を 16 個のビット並びでデジタルデータとして記録し扱うため、15 ビットでは何を表現・表示(情報自体の意味)をすれば良いのか困ってしまうことになる。

このような場合、最初のビットが消えたと知っていれば、単純に「0」か「1」のどちらかを入れれば原本情報を再現できるが、果たして「0」を入れた並びと「1」を入れた並びのどちらが原本なのか判定する手段がない。(「誤り訂正符合」を持たせていない場合)

3. 情報セキュリティ技術の原点と秘密分散技術

原本情報が変換されたり、ビットが欠落することは、非常に大きなダメージをデジタルデータに与える。すなわち、情報システム、情報社会、情報セキュリティにとって、極めて深刻な事態を引き起こす要因となりうる。

具体的なダメージは次の 2 点、すなわち、

●原本のビットが改竄されると、原本情報が利用できない
●原本情報のビットが欠落すると、原本情報が利用できない

なのであるが、この特性を逆手に取ると、

●原本情報に変換を加えると、原本情報が悪用されない
●原本情報のビットを欠落させると、原本情報が悪用されない

ということになる。これが、まさにデジタルデータに関する情報セキュリティの原点とも言うべき原理であり、前者の「変換を行い情報を保護する技術」を一般に暗号技術と言い、後者の「ビットを分散させて情報を保護する技術」が、本報告で中心的に扱う秘密分散技術となる。

暗号は、古くはシーザー暗号から現代暗号まで広範で様々な研究が行われてきた。多くの戦争においては、その暗号の優劣と、解読手法の発見が、戦局を一変させてきたという歴史もある(エニグマやパープル暗号など)。一方、秘密分散技術は、印鑑と陰影の関係や、古くは中国の戦国時代の「軍割符」、日本も歴史で関わる「勘合貿易の勘合符」、ヨーロッパでもギリシャ語で「割符」を意味する単語(英語圏に入り symbol になったという説あり)があったり、現代の小切手帳と小切手の関係や契約書の割印であったりと、人類の生活・歴史に密着してきた情報の運用管理手法と言える。

さて、暗号の特徴は、

a) 解読までの時間をかせげる
b) 鍵をきちんと管理すれば、複数の情報を集約的に管理できる
c) 鍵管理の依存度が高い情報管理手法
d) 善良なる利用者・管理者だけが利用している前提

と言える。一方、割符が暗号と比べてユニークなのは、軍の指揮権を管理する軍割符も勘合貿易の勘合符も、外部からの攻撃や内部の反乱等も想定した、非常に厳しいリスク管理に直面している場面で用いられた手法・道具であることである。この場合、割符を持っていることで正当な権限者とみなし(認証)、割符を開示しあい、合体させた際にはじめて復元される情報によって、その内容の原本性(改竄防止)を保証し、その権限が乱用されないよう権限を分散(相互牽制)させたと言える。よって、

a) 性悪説に対処する手法であること
b) 割符を保有する者を、正当な権限者とみなした(認証機能)
c) 原本情報の改竄を防止
d) 原本情報を関係当事者複数で相互牽制して管理

といった特長が、秘密分散技術のルーツとなる「割符」にはあったわけである。どれも現代社会、IT社会にとって大切な機能であることは間違いなく、このような原理的特性を持つことが、我々がタスクフォースの課題として取り上げた一因となっている。

さて、デジタルデータを対象とする割符=秘密分散技術においては、新たに極めて重要な特性が出現している。すなわち、**「原本情報をビットレベルで分割し生成した部分集合単独では、原本情報を導き出せないため原本情報ではないと判断できる」**ということである。この原理的特性は、変換技術だけでは達成できない大きな特性で、例えば原本が個人情報であっても秘密分散されたものは個人情報とは認められない、原本が機密情報であっても秘密分散されたものは機密情報とは認められない、というような法的見解が出る要因となっている。このことは、暗号技術に対しては**「個人情報は暗号化されているかどうかを問わない」**という見解が出ているのとは好対照である。

以上の特性の違いは、どちらがいい・悪い、と言った次元の話ではなく、今後、暗号技術と秘密分散技術をうまく組み合わせた仕組みによって、多くの情報セキュリティシステムの安全性や安心感が向上していくという根拠となりうるものであろう。

4. 秘密分散技術の安全性と技術要件のあり方

秘密分散技術の典型的かつ原始的な処理では、原本情報のビット列を、ビット単位で分散して、いくつかのばらばらにされたビットの塊(「割符ファイル」と呼ぶ)を生成していく。このような処理の場合の安全性を考えてみたい。

例えば、1000 ビット(125 バイト)の原本情報をビット単位でばらばらにして 2 つの割符ファイルを生成したと仮定しよう。当然、生成される割符ファイルは 1000 ビット未満である。復元するための仕組みもあると仮定した場合、手元に 500 ビットの割符ファイルがあれば、残りの 500 ビットの割符ファイルさえ入手できれば原本情報を入手できるはずである。この時、原本のビット長(1000 ビット)も、生成した割符ファイル(部分集合)の数(2 つ)も、復元する仕組みの情報もあるため、残りの 500 ビットの未入手の割符ファイルを作り出せれば、原本情報を入手できるのだが、この時、どのくらいの試行錯誤をしなければならないのだろうか?

この作業の困難さを表現する際に、情報セキュリティの世界で良く用いられるモノサシが**計算量的安全性**という表現である。

さて、ここで、秘密分散法と秘密分散技術について整理しておきたい。世の中で秘密分散技術を説明する際に良く登場するのが、秘密分散法という数学(暗号)理論である。この理論のベースは、中学校で勉強する連立方程式であり、「未知の値が有る場合、その未知の値を導き出すのに必要な数の関係式が無いと、未知の値が導き出せない」、という単純な仕組みで説明されることが多いが、この仕組みにより暗号理論の世界で言う「完全秘匿(パーフェクトシークレシー)」を実現できるものである。しかしながら、本稿では、秘密分散技術は『割符』をデジタルデータの世界に適用したものと考えており、「原本情報をビットレベルで分割し生成した部分集合単独では、原本情報を導き出せないため原本情報ではないと判断できる」という原理的特性を充たしていれば、秘密分散法のみならず他の方法を使っても秘密分散技術を実現できるとの立場を取る。従って、本稿においては、秘密分散技術は現実のデジタルデータをビットレベルで分割していくものなので、(完全秘匿を実現できる秘密分散法を使わないような)単純な仕組みの場合は、欠落した部分を補っていけば解を見出せる可能性がゼロではなく、計算量的な安全性を持つと言うのが正しいものと考える。つまり、未知の割符ファイルを何とか作り出せれば、原本復元の道が開けるということである。ただし、繰り返しになるが、完全な秘密分散法を実装した秘密分散技術を用いれば完全秘匿することも可能であり、秘密分散技術として秘密分散法を否定するものではない。

ちなみに、現代暗号の代表格である公開鍵暗号や共通鍵暗号の標準 AES は、コンピュータの性能の進化に合わせて、推奨している暗号強度(前述の計算量)を変化させていっている。何故ならば、そうしないと暗号の重大な役割である「解読までの時間を稼ぐ」ことができなくなってしまうからである。概ね、強度の見直しは 3〜5 年くらいの周期で行われ、世界中の暗号を利用したシステムでは、定期的に暗号の入れ替え作業が必要となっているという現実は理解しておく必要がある。

再び、秘密分散技術に戻る。先の例では、デジタルデータは、0 と 1 で構成され、更にそれらが 500 ビット並ぶということは、その組み合わせの数は、2 の 500 乗(指数関数を用いて表現する)である。原本情報が 10000 ビット(1.25K バイト)であれば 2 の 5000 乗となる。どの程度の時間が計算にかかるかはここでは言及しないが、秘密分散技術においては、原本情報がある程度大きければ、相当なレ

ベルの計算量的安全性を確保できるということは言えるだろう。これにより、暗号に特徴的な強度の見直しという難題からは少なくとも逃れることができる、ということができそうである。また、前述の秘密分散法を使う場合については、仮に完全な実装を行うことができた場合、計算量的安全性は無限大、すわわち(現実的な善し悪しを無視するならば)完全秘匿が実現できると考えてよいだろう。

現実には、秘密分散技術を外部評価する際に有効な攻撃手法が有識者等の間で認知されていないこともあるため、上記の数字をそのまま安全性の根拠とするわけにはいかないが、秘密分散技術の原理的な特性から考えられる解読手法の最有力候補が「総当り」という手法であるため、前述の数値が基本的なモデルとなることは間違いないと思われる。

すなわち、**秘密分散技術における安全性は計算量的安全性と理解すべきものであり、技術的な側面においても計算量的安全性を確保するための要件の実現が最優先される**べきものである。

5. 秘密分散技術に関する利活用のあり方

先の秘密分散法だけではなく、数学的な暗号の世界において理論上は「完全秘匿」が実現できるケースは多い。しかしながら、実際に市場に流通する暗号商品に、そのような機能・性能を保証したものはない。これはどういうことだろうか?

完全秘匿とは、どうやっても解読できない情報秘匿レベルを指す。情報量を根拠とした理論や、秘密分散法、完全な実装ができているのであれば一般に暗号理論として正当な評価を受けているものは、理論上完全秘匿が実現できている(はずである)。守って欲しい情報が、完全秘匿されるのは良いことのように感じるが、果たして本当にそうなのだろうか?

実社会は実に複雑である。様々な考え方の人がいて、様々な活動をしている人がいる。故意であっても、そうでなくても、情報の完全秘匿が実現されている仕組みが一般に流通するということは、社会全体から見たときに大きな脅威になる可能性がありうるのである。例えばテロリストが完全秘匿できる暗号技術を使っていたらどうなるだろうか? 捜査当局が情報を入手しても絶対に暗号を解くことができないという状況は明らかに好ましくないだろう。つまり、ここにその時代背景に応じた適切なレベルの情報秘匿を実現できる技術だけが世に出せる理由があるのである。つまり、完全秘匿ができるということは、考えようによっては社会保障の脅威となる「化学兵器や核関連技術」にも匹敵する技術になってしまう可能性があるということである。

以上から、理論を忠実に実装したことで完全秘匿を実現していることを証明できる暗号技術や秘密分散法自体は一般市場に容易に流通させるべきではなく、ここに計算量的安全性を特徴とした秘密分散技術の社会的有用性の根拠を見出すことができる。また、本稿において、秘密分散技術を実現する方法として秘密分散法以外を認めるのも同様の理由による。

このような観点から秘密分散技術を見直すと、別の特徴を見つけることもできる。例えば以下のようなものである。

a) 数学理論等を実装したのではなく、単純な情報処理技術であり、計算量的な安全性で説明できるため、社会保障上の危険な技術にならない
b) 愉快犯が攻撃しようとした際に、非常に手間のかかる仕組みを容易に構築できる可能性がある
c) 原本情報をビットレベルで分割しているので、個々の割符ファイル単体からは個人情報等の原本の持つ意味のある情報が流出しない
d) 一般の理解を得られやすい処理である

もちろん、このような特徴も念頭において利活用シーンを考えるべきことは言うまでもないだろう。

さて、計算量的な安全性を特徴とする秘密分散技術の利活用において、最もやってはならないことは何だろうか?

これは明白である。複数に分割されていることが計算量的安全性を担保しているならば、**複数に分割されたものを容易に一箇所に集められるような利活用をしてはならない**、ということに尽きる。これは、暗号化を使った場合、暗号化されたデータと解除用パスワードを一緒に管理してはならない、

という運用に近いため誰でも容易に想像できるだろう。つまり利活用段階においては、いかにこの点をクリアしつつ、使いやすいシステムに組み上げられるか、が問題になるということなのである。例えば、現実問題としては、分割して管理するのをユーザが嫌がる傾向があるため、ユーザに分割した場所がわからないようにシステムで管理するような機能を実現した場合、システムの管理情報をハッキングすれば分かれたものを一箇所に集めるための情報を簡単に入手できるという問題がおきる。暗号でも同様だが、結局システムを提供する側がユーザビリティと情報セキュリティのバランスをどのように保つような機能ポリシーとし、導入する側がどのような運用ポリシーにするか、という問題の好例であろう。

6. ガイドラインについて

これまでの記載をさらにわかりやすく説明するために、情報セキュリティ技術としての秘密分散技術として大きく捉えるのではなく、より具体的にファイルを保存したり移送したりする場合のリスクマネジメント手法として秘密分散技術を捉え、技術的な観点および利活用における観点からガイドラインを作成した。別紙として添付するので参照されたい。

7. 法的提言

牧野総合法律事務所弁護士法人の牧野二郎弁護士から、秘密分散管理技術(電子割符技術を利用した情報管理)に関する法的な意見書をいただいた。別紙として添付するので参照されたい。

8. 終わりに

今回は、秘密分散技術の利活用検討を行うにあたり特定の会社、特定の技術に寄らない一般的な秘密分散技術を対象とし、基本的なガイドラインの作成と法的提言の獲得を行うことができた。今後は、今回記載から漏れた技術の調査や秘密分散技術の規格を ISO に登録するような動きをしていくことで秘密分散技術、ならびに情報セキュリティ技術の発展に寄与できるものと考えている。

また、本タスクフォースにおける検討と平行して、経済産業省委託調査『中小企業等製品性能評価事業・情報セキュリティ技術を使った情報利活用基盤構築に関する共同研究と実証事業』を財団法人日本情報処理開発協会・次世代電子商取引推進協議会および各共同研究事業者と共に実施している。採択された 4 案件のうち 2 案件が本報告の秘密分散技術に関連するものであり、実際の利用や活用を前提とした実証を行うことができたので、そちらの報告書も参考にしつつ、秘密分散技術を利活用したビジネスを検討していただければ幸いである。

以上

タスクフォースメンバー名簿

（敬称略）

№	役　割	氏　名	会　社　名
1	メンバー	保倉　　豊	グローバルフレンドシップ株式会社
2	メンバー	高橋 和博	株式会社テプコシステムズ
3	メンバー	雨車　美和	デジタルアース株式会社
4	メンバー	大竹　正敏	株式会社トッパン・エヌエスダブリュ
5	メンバー	垣内　伯之	日本情報処理開発協会
6	オブザーバー	西野　敏行	日立ビジネスソリューション株式会社
7	事務局	合原　英次郎	次世代電子商取引推進協議会
8	事務局	山崎　幸男	次世代電子商取引推進協議会

秘密分散に関する技術ガイドライン
および
秘密分散技術利活用に関するガイドライン

平成 22 年 3 月

次世代電子商取引推進協議会

目　次

1. はじめに 1
2. リスクマネジメントから見た秘密分散技術 2
3. 秘密分散技術を実現するソフトウェアプロダクトにおける必須要件 4
4. 秘密分散技術を実現するソフトウェアプロダクトにおける任意要件 8
5. 秘密分散技術を利活用するシステムにおいて考慮すべき必須要件 10
6. 秘密分散技術を利活用するシステムにおいて考慮すべき任意要件 12
7. 秘密分散技術の具体的活用例 13
8. 代表的な秘密分散技術について 16

1. はじめに

まず、本ガイドライン作成にあたり、秘密分散技術を、情報セキュリティ技術として先行し社会的に深く認知・利活用されている暗号技術に敵対したり置き換えるものではなく、暗号技術を補完するもの、あるいは暗号技術と組み合わせることで相乗効果をもたらすものとして捉える方針とした。これは、この方がより現実的なガイドラインとできると判断したためである。

そもそも、暗号が数学理論をベースとしているのに対し、秘密分散技術は、人類の英知とも言える『割符』の考え方を現代のデジタルデータに適用した技術であり、数学理論に基づく完璧な安全性よりも計算量的安全性を重視したものである。また、「原本情報をビットレベルで分割し生成した部分集合単独では、原本情報を導き出せないため原本情報ではないと判断できる」という原理的特性から、例えば原本が個人情報であっても秘密分散されたものは個人情報とは認められない、原本が機密情報であっても秘密分散されたものは機密情報とは認められない、ということが言えるため、逆に「複数に分割されたものを容易に一箇所に集められる場合秘密分散しているとは言えない」という利活用上の大きな制約が発生するはずである。しかしながら、何がどう問題なのか、という統一的な見解が存在せず、各社ばらばらにシステムコンセプトを考え、また運用しているのが現実であり、これにより少なからず利用するユーザが導入メリットを感じ得ない、あるいは運用が混乱する、ということが起こっていると聞く。

そこで、上記方針に従い、より具体的な利活用シーン、例えばファイルを保存したり移送したりする場合のリスクマネジメント手法の１つとして秘密分散技術を捉え、その上で秘密分散技術を現実のシステムとして実装する場合の技術的・機能的な制約事項等、あるいは利活用における運用上の制約事項等をまとめガイドラインを作成することとした。本ガイドラインにより、実際に秘密分散技術を実現するソフトウェアライブラリやそのソフトウェアライブラリを組み込んだソフトウェアプロダクトを開発したり、ソフトウェアプロダクトを活用してサービスを提供する際の一助となれば幸いである。

なお、ソフトウェアプロダクトやサービスを提供する者は、それぞれ外部検証やフィールドテスト等を行う等の、提供者としての確認を行い市場に技術やサービス等を提供することを前提とする。また、あくまで情報を分割して運用管理する手法であり、暗号技術の補完的役割であることと、社会的安全保障上の観点等を勘案し、数学的理論を実装したアルゴリズムで、理論上完全秘匿が証明できる暗号技術は、本ドキュメントの対象範疇には組み入れないことを予めお断りしておく。

2. リスクマネジメントから見た秘密分散技術

一般に暗号を利用する場合最も重要とされていることは、暗号解除のためのパスワードを容易に想像できないものとしたり、他のパスワードと異なるものとしたり、パスワードをメモに留めたりしないこと、とされる。また、「個人情報は暗号化されているかを問わない」という非常に厳しい見解もあることから、例えばデータを暗号化して保管する場合、情報漏洩リスクは次のケースで最大化する可能性があると考えることができる。

- パスワード(鍵)が第三者において容易に想像または取得できる
- 個人情報データを暗号化したファイルが容易に第三者の手に渡る

これらは、パスワード(鍵)または暗号化されたファイル、またはその両者の運用・管理におけるリスクであることは一目瞭然である。さて以上の問題を解決しリスクを低減するためにはどうすればいいだろうか? その 1 つの解が、本ガイドラインで取り上げる秘密分散技術の導入である。上記の問題に秘密分散技術を適用してみると、

- パスワード(鍵)を秘密分散し 2 つ以上に分けて管理する
- 個人情報データを秘密分散し 2 つ以上に分けて管理する

となる。これにより、「原本情報をビットレベルで分割し生成した部分集合単独では、原本情報を導き出せないため原本情報ではないと判断できる」という原理的特性から、パスワード(鍵)や個人情報を含むデータを秘密分散した場合、秘密分散されたそれぞれのファイルやデータはパスワード(鍵)とは認められず、また個人情報とは認められない。すなわち、秘密分散技術を適用することにより、暗号の場合発生していた 1 箇所での運用・管理リスクを複数箇所での運用・管理リスクに置き換えることで、リスクの分散を図ることができる、と言うことができるだろう。もちろん忘れてはならないのは、秘密分散技術を適用することにより、複数箇所で管理するための運用コストおよび運用上のリスクが新たに発生していることであり、これが一概に秘密分散技術が良い、と言い切れない理由ともなっている。つまり、対象とするデータや運用コストから、暗号と秘密分散技術を適切に使い分け、あるいは組み合わせて使うことが現実には必要となる、ということである。が、少なくとも暗号しか選択肢がないよりは秘密分散技術も選択肢の中に入れられるようになることで、ユーザは大きな安心を得られる可能性が増える、ということが重要なのである(ユーザにとっては、暗号化+秘密分散、暗号化のみ、秘密分散のみ、の 3 つの選択肢が考えられる)。

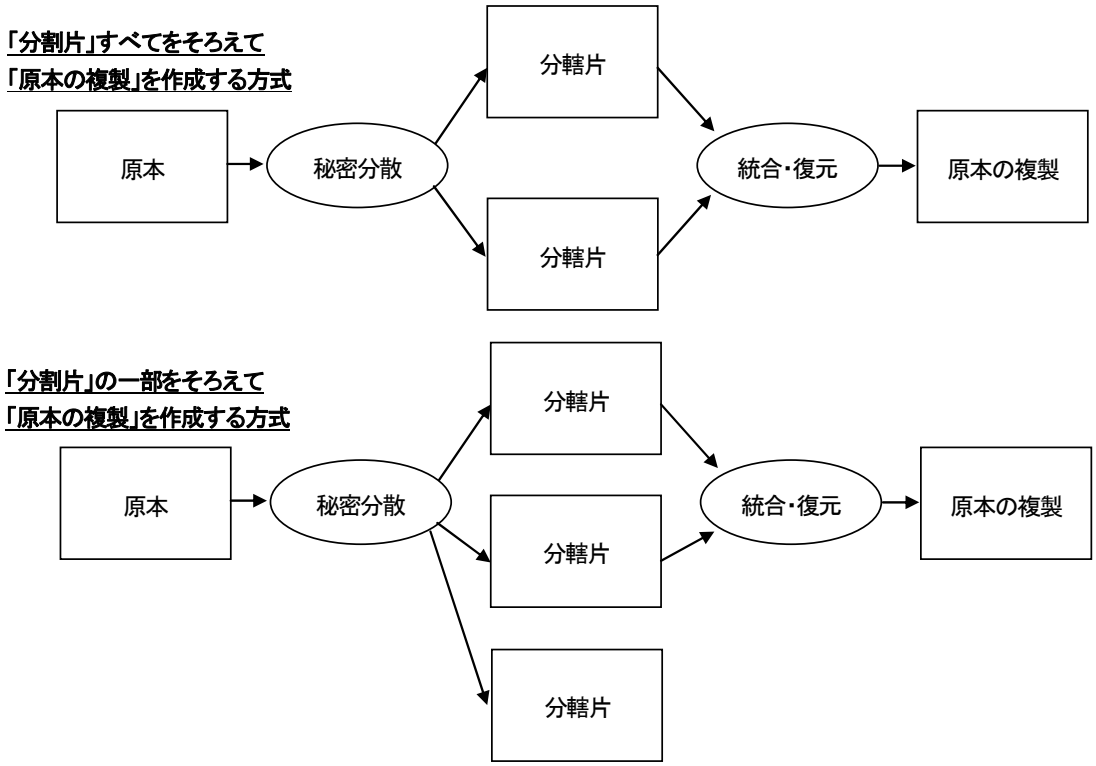
さて、リスクを分散する効果を得られる秘密分散技術ではあるが、実際に利活用するにあたり認識しておくべきリスクは何だろうか? これは簡単である。「原本情報をビットレベルで分割し生成した部分集合単独では、原本情報を導き出せないため原本情報ではないと判断できる」という原理的特性と、計算量的な安全性を実現していることから、

- 複数に分割されたものを容易に一箇所に集められるようなソフトウェア実装や運用が行われているケース

- 計算量を少なくできるようなソフトウェア実装や運用が行われているケース

の 2 つが最も大きなリスクとなりうると考えて良いだろう。以下、この 2 つのリスクをいかに少なくするか、という観点で論を進める。

説明においては、下図のように、秘密分散技術適用前のデータそのものを「原本」、秘密分散技術適用前のデータとまったく同一の価値（ビット列）を持つデータを「原本の複製」、秘密分散技術適用後のそれぞれのデータを「分割片」と呼び、秘密分散技術(採用)を名乗るための必須要件および任意要件の説明を行っていく。なお、分割(分散)方式として、「分割片」すべてをそろえて「原本の複製」を作成する方式(秘密分散法では「n-out-of-n 分散方式」などと呼ばれる)と「分割片」の一部をそろえて「原本の複製」を作成する方式(秘密分散法では「k-out-of-n 分散方式」などと呼ばれる)があるが、本稿では詳細説明は行わない。



3. 秘密分散技術を実現するソフトウェアプロダクトにおける必須要件

1	［機密性］ ● 基本アルゴリズムを公開しても単独の「分割片」から「原本」の一部すら容易に推測できないこと、または推測するためにかかる計算量を例示できるようにすること

【解説】

■ 秘密分散技術の肝はデータの分割または分散格納であり、分散格納されたおのおのは例えば個人情報ではないという判断の元に容易にアクセスできる場所に格納される可能性がある。このことは、愉快犯などにより執拗なアタックを受ける可能性を考慮せざるを得ない。よって、コアとなる基本アルゴリズム(基本アルゴリズムそのもの、または基本アルゴリズムを実装したソフトウェアプロダクト、または基本アルゴリズムを実装したソフトウェアプロダクトライブラリ。以下も同様の意味で使用)は原則公開、または公開請求があれば公開できる程度に安全性に問題がないものである必要があり、これにより、適切に「分割片」を分散させて管理していれば基本アルゴリズムが公開されていても「原本の複製」を作成することは事実上不可能であると言えるようにしておくべきである。また、ハッカーがプログラムを解読することは良くあることと考えれば、基本アルゴリズムが期せずして公開されても安全なレベル、ということが二重に求められる。

■ ただし、ファイルの付帯情報の管理など、基本アルゴリズムとは直接関係ない情報の操作に関しては公開不要である。例えば、アプリケーションソフトウェアプロダクトとして秘密分散技術を提供する場合、どの「分割片」を組み合わせるか、をいちいちユーザが指定するのはユーザビリティ上問題がある。「分割片」の外に付帯情報として組合せ情報を管理する仕様をアプリケーションソフトウェアプロダクトが提供することは可能であり、この仕様を公開する必要はない。

■ 基本アルゴリズムが公開されていることが前提となるが、ペアとなる「分割片」相当のデータをランダムに作成し、総当りで「原本の複製」を作成するようなハッキングを行う場合、どの程度の計算量でどの程度のデータが推測可能となるのか、を例示できるようにすべきである。例えば、『xxx 方式の場合、xx Kbyte のファイルを均等サイズで秘密分散した場合、「分割片」の 1byte を推測するために 10 の xxx 乗回以上の総当り計算を行わなければならない』、などのような形で公開すれば、少なくともユーザは xxx 年は大丈夫という目安を得ることができる。

2	［機密性］ ● 「分割片」は 2 つ以上であること ● 統合・復元に必要な個数の「分割片」が同時に容易にアクセスできる場所に格納されないこと

【解説】

■ 2 つ以上に「原本」を分割または分散を行うことができればよく、これを実現するための基本アルゴリズムは何を使ってもよいものとする。一般に閾値秘密分散法が使われることが多いが、結果的に秘密分散技術の条件を充たすことができれば、閾値秘密分散法を使わなければならないということはない。ここは、秘密分散技術を実現する各企業の腕の見せ所となるだろう。ただし、完全秘匿を実現するようなアルゴリズムの採用に関しては、反社会的勢力に使われる可能性も考慮した上で実装レベルを検討すべきである。

■ 「分割片」をいくつ揃えると「原本の複製」を作成できるか、は問わない。例えば、2 つに分割したものをすべてそろえると「原本の複製」を作成できてもよいし、3 つに分割したもののうち 2 つで「原本の複製」を作成できてもよい。

■ 統合・復元に必要な複数の「分割片」が同時に容易にアクセスできる場所に格納されてはならない。容易にアクセスできるということは、秘密分散技術においては簡単に統合・復元できることを意味するためである。複数の「分割片」をいかに管理するか、はアプリケーションソフトウェアプロダクト側で検討すべきものであり、基本アルゴリズムで原則カバーしてはならない。これは、管理情報をハッキングすることで「原本」の情報を取得することを応用レベルで留めるためである。ただし、十分に管理情報に対するハッキング対策を施すことが可能な場合には基本アルゴリズムでカバーすることを否定するものではない。

3	［可用性］［完全性］ ● 正しい「分割片」の組合せからは正しい「原本の複製」を作成できること ● 正しくない「分割片」の組み合わせからは正しい「原本の複製」が作成できないこと ［真正性］［信頼性］ ● 正しい「分割片」の組合せから正しい「原本の複製」を作成した場合、それは「原本」とまったく同一の価値（ビット列）を持つこと

【解説】

■ 「分割片」を改竄した場合、「原本の複製」が作成できない、または「原本の複製」とは異なるデータを作成するようなアルゴリズムを採用している必要がある。前者のアルゴリズムの場合、作成できることが「原本」と同様であることを証明できるような仕様となっている必要がある。後者の場合、「原本」とのデータ比較により「原本の複製」であることを証明するような仕様を充たしている必要があり、現実には改竄を検知した場合は統合・復元処理を止めるべきである。なお、後者については、統合・復元しつつ問題があったことを履歴として出力できるような仕様を充たすことで、システムとして、そのまま間違ったデータを統合・復元してわざと問題を発生させる、という仕様もありうるはずであるが、一般的には前者の実装を推奨する。

■ 正しい「分割片」の組合せは「原本の複製」が正しく作成できることをもって証明される必要があるが、アプリケーションソフトウェアプロダクトとして正しい「分割片」の組合せがどれであるか管理してもよい。

4	[機密性][完全性][可用性] ● 「分割片」内には自他の「分割片」に関する情報や「原本」の情報を含まないこと ● 「分割片」の組合せ順番は任意であること ● 同一の「分割片」が存在しないこと、または同一の「分割片」が出現する確率を明示または開示要求があれば開示すること ● ゼロ byte ファイルまたは小さなファイルに対しても総当り攻撃に対し十分安全な配慮を行うこと

【解説】

■ 基本アルゴリズム公開を前提とした場合、自サイズや名称、対となる「分割片」の名称やサイズ等、ハッキング時の総当り計算量を少なくするような情報を基本アルゴリズム上含まないようにしておく必要がある。例えば、対となる「分割片」のサイズが十分小さいと判明した場合とまったくわからない場合では、総当り計算量が大幅に変わってくるため、このような計算量を少なくする方向に働く情報は含まないことが重要である。

■ 「原本の複製」を作成する時に「分割片」の組合せに順番が存在する場合、順番に関する情報を元にハッキングされる可能性が高まると考えられる。組合せの順番に関する情報を「分割片」に保持してはならない。

■ 何度か秘密分散処理を行った場合、同一の「分割片」が生成される場合は、特定の「原本」に対し固定の「分割片」を作ってしまう可能性がある。乱数を使うアルゴリズムの場合、乱数の精度等から同一の「分割片」が出現する確率を明示または開示できるようにしておく、同一の「分割片」が事実上出現しない乱数を使用する、使い捨ての乱数を使う、などの対策が考えられる。

■ ゼロ byte ファイルまたは小さなファイルを秘密分散した場合、「分割片」が小さいため総当り攻撃に弱くなる可能性がある。よって、安全なサイズまでノイズを入れるなどの配慮を行う必要がある。

4. 秘密分散技術を実現するソフトウェアプロダクトにおける任意要件

1	［可用性］ ● 異なるプラットフォームをサポートする場合、正しい組合せの「分割片」の組からは、異なるプラットフォームにおいても同一の「原本の複製」が作成されること

【解説】

■ プラットフォームが異なるからと言って異なるタイプの「分割片」を作ることは実運用に支障を来たす。同一バージョンのアルゴリズムから作られる「分割片」はいかなるプラットフォームであっても同一の「原本の複製」を作成できることが望ましい。

■ ただし、組込み機器とハイパフォーマンス PC のように、処理性能やリソースに大きな差があり、異なるプラットフォームであっても同じ結果となる、という形とした場合、性能が悪いプラットフォーム用に速度を重視したアルゴリズムを採用する、ということを否定するものではない。アプリケーションソフトウェアプロダクトとしてのトータル性能を考慮したアルゴリズム採用を考慮すべきである。

2	［可用性］［真正性］ ● すべての「分割片」をそろえなくても統合・復元できる機能をサポートすること ● すべての「分割片」をそろえなくても統合・復元できる機能をサポートする場合、いくつかの「分割片」の組み合わせパターンが存在しても作られる「原本の複製」は同一であることを保証すること

【解説】

■ N≧2 の時に N 個の「分割片」を作り、N 個の「分割片」すべてで「原本の複製」を作成する機能だけではなく、N≧3 の時に N 個の「分割片」を作り、N-1 個以下の「分割片」で「原本の複製」を作成する機能をサポートすることが望ましい。

■ 例えば、すべての「分割片」をそろえなくても統合・復元できる機能をサポートした場合、例えば 3 個のうちの 2 個で「原本の複製」を作成することが 3 パターン可能であり、それぞれでき

た「原本の複製」を比較するとまったく同一のデータである。つまり、「分割片」が改竄されていない証明と「原本の複製」が正しく作成されたことを証明できる仕掛けができあがる。

■ また、3 個の「分割片」を、例えば日本とアメリカとヨーロッパのデータセンタに分散して格納した場合、どこか 1 箇所のデータセンタが地震などで使えなくなっても残りの 2 つで「原本の複製」を作成することが可能となる。これは一種のディザスタリカバリを実現したと見なすことが可能であろう。

3	［可用性］ ● 「分割片」のサイズ配分を可変にできること

【解説】

■ 例えば、均等分割(1:1)のみでは対になる「分割片」のサイズがわかるため、総当り計算量を少なくできる可能性がある。任意サイズに分割でき、かつその分割配分が「分割片」に情報として格納されていないことが望ましい。なお、任意サイズに分割した場合、「分割片」が十分に小さいと総当り攻撃に対し脆弱になる可能性がある。安全性に考慮して、最小サイズの考慮を行うべきである。

4	［可用性］ ● 付帯情報を安全に追加できること

【解説】

■ 秘密分散はデータを分散格納することが肝ではあるが、パスワード等を設定できるようにするなどして更に安全度を高めることを考慮すべきである。パスワード等の付帯情報を付加できるような仕様となっていることが望ましい。

5. 秘密分散技術を利活用するシステムにおいて考慮すべき必須要件

1	［可用性］ ● 「原本」を指定し「分割片」をシステム的に格納する方法を提供できること

【解説】

■ 基本アルゴリズムには「原本」の指定方法および「分割片」を実際に作成し格納する方法は含むべきではない。しかしながらアプリケーションソフトウェアプロダクトとしてはユーザビリティを考慮して「原本」の指定方法および「分割片」の格納方法を検討し実装すべきである。

■ 「分割片」については、例えば同一 HDD 内に格納した場合「分割片」であっても容易に探し出し「原本の複製」を作成することができる。運用も鑑み、異なる場所に格納する方法を検討し実装する必要がある。

2	［可用性］ ● 「分割片」をシステム的に組合せ指定し「原本の複製」を格納する方法を提供できること

【解説】

■ 基本アルゴリズムには「分割片」の組合せ方法および「原本の複製」を作成し実際に格納する方法は含むべきではない。しかしながらアプリケーションソフトウェアプロダクトとしてはユーザビリティを考慮して「分割片」の組合せ指定方法および「原本の複製」作成方法を検討し実装すべきである。

3	［可用性］ ● 「原本」削除と「原本の複製」の上書きを制御できること

【解説】

■ 「原本」の削除と「原本の複製」の上書きはアプリケーションソフトウェアプロダクト側で制御すべきである。

■ 「原本」の削除をシステム的に行う場合、HDD 上で削除しても容易に統合・復元が可能である。完全に削除するような仕掛けも検討し可能であれば実装すべきである。

4	［責任追跡性］［否認防止］ ● 一連の操作および結果を履歴として蓄積する機能を付加すること

【解説】

■ 「分割片」の作成、「原本」の削除、「原本の複製」等、一連の操作および結果については、履歴として蓄積する機能を実装すべきである。また、開示要求に対し、履歴を開示できるような機能を実装すべきである。

6. 秘密分散技術を利活用するシステムにおいて考慮すべき任意要件

1	［可用性］ ● 付帯情報を追加・管理すること

【解説】

■ ユーザが必要な「分割片」の対を記憶し、それを指定して「原本の複製」を作成するのがもっとも安全だが、ユーザにとっては負担が大きな作業となる。システムとして付帯情報を管理し、安全度を下げない程度にユーザ負担を軽減するような機能を実装することを推奨する。

■ 付帯情報として、例えば統合・復元可能な時間、地域の情報、統合・復元回数、統合・復元履歴、作成者、統合・復元可能なユーザ情報など、様々な情報が考えられる。これらをどのように追加・管理するかでシステムの色も使い勝手も大きくかわってくることになる。

2	［可用性］［信頼性］ ● 第三者機関との連携

【解説】

■ すべての「分割片」をそろえなくても統合・復元できる機能をサポートした場合、3 つを格納する場所をユーザが準備することはなかなか難しい状況である。例えば 3 つのうちの 1 つ以上を第三者機関に預けられるようなサービスとの併用ができるような構造を取ることを推奨する。

7. 秘密分散技術の具体的活用例

ここでは、秘密分散技術の具体的活用例を示す。

(1) 情報漏洩対策

2 つの「分割片」を作成し、それぞれ別の場所に管理することにより情報漏洩対策を行うような活用は、秘密分散技術活用の基本中の基本である。例えば、2 つの「分割片」を作成し、2 つで統合・復元できるようにした場合、USB メモリを使った暗号化と同じ秘匿目的での使用が可能である。特に、効果が高いのは、元データが個人情報等の場合であり、秘密分散したものは元の価値を持たない、という特性を利用できるケースである。

［活用例］

- ノート PC の HDD に 1 つの「分割片」、USB メモリにもう 1 つの「分割片」を入れ、ノート PC=データ移動時は USB メモリを取り外すことで 2 つの「分割片」の同時紛失を防止し、目的地到着後 USB メモリを挿入して「原本の複製」を作成することができる。
- 「分割片」の 1 つをメールに添付し、もう 1 つを CD-R に焼いて相手先に送付したり DC に格納してダウンロードできるようにすることで、相手先で「原本の複製」を作成することができる。

［応用例］

- 2 つの「分割片」が目的地でのみ同一の場所に存在する=「原本の複製」を作成したということを証明するために、2 つの「分割片」の移動経路を GPS 装置でトラッキングし地図上にマッピングするようなソリューションを提供することができる。(経済産業省委託調査『中小企業等製品性能評価事業・情報セキュリティ技術を使った情報利活用基盤構築に関する共同研究と実証事業』において、デジタル・アース株式会社が実施した「電子的割符のトラッキング情報運用管理プラットフォームの開発」がこれに相当する)
- 相手先とのデータ通信を、同時に 2 つの通信経路を使い、かつそれぞれは「分割片」に相当するデータとすることで、同時に 2 つを盗聴できなければ解読できない通信を実現可能である。
- 暗号化したファイルを更に秘密分散することで、非常に高い安全性を確保できる。

(2) データバックアップ・ディザスタリカバリ・BCP

3 つの「分割片」を作成し、それぞれを別の場所で管理し、任意の 2 つの組み合わせで「原本の複製」を作成するような運用は、情報漏洩対策と同時に、1 つを紛失しても残り 2 つから統合・復元できるというデータバックアップやディザスタリカバリ、BCP の機能を提供できる。

［活用例］

- 3 つの「分割片」を格納する場所を、例えば本州、北海道、九州の DC とすることで、地震などの天災時におけるディザスタリカバリや BCP の用途として活用できる。

［応用例］

- 個人情報たる卒業写真データを 3 つの「分割片」に分け別々の DC に格納し、一時的に写真データを参照するための仕掛けを提供することで、大切な写真データを天災から守るためのシステムを提供するソリューション。(経済産業省委託調査『中小企業等製品性能評価事業・情報セキュリティ技術を使った情報利活用基盤構築に関する共同研究と実証事業』において、ヤノ電器株式会社が実施した「クラウドシステム構想における大容量データの安全保管と活用環境整備」がこれに相当する)
- 遺言書の電子情報を秘密分散し、3 つの「分割片」をそれぞれ、本人、第三者預かり所(データセンタ)、公証人役場等で管理し、必要な時には 3 つのうち 2 つの組合せで統合・復元する。これを異なる組み合わせで実施し、結果が同じとなることで元の「分割片」が改竄されていない=統合・復元された「原本の複製」が改竄されていない、という内容証明を実施することができる。かつ、それぞれの「分割片」は個人情報でも機密情報でもないので、より安価な DC や設備において預かることができる。

(3) 認証・セキュアな鍵管理

機密文書の暗号化を行った際に使用した暗号鍵の保管方法として、秘密分散技術を使うことで、鍵の分散管理を簡単に実現できる。暗号化との組み合わせとしては最もオーソドックスな使い方と言える。

［活用例］

- パスワードを秘密分散して複数の人に「分割片」として渡し、複数人の合意でなければパスワードがわからないようにする。あるいは、1 つをシステムで管理し、もう 1 つをユーザに渡す方法もある。

［応用例］

- 複数人の合意によるログイン認証の実現。さらに進んで、3 つのうち 2 つ、4 つのうち 3 つで統合・復元できる、などの設定を組織構造に合わせることで、役職レベルに応じたログイン認証や鍵の分散管理を行うことができる。
- サーバ・クライアント間において暗号鍵を受け渡しを行うことで安全な通信を行うような場合、その暗号鍵を秘密分散しその「分割片」を交換することで、相手認証と鍵の共有を同時に行うようなシステムを実現可能である。
- 秘密分散を行うたびに異なる「分割片」ができる場合、この特性を利用して、ログイン成功の度に次回に使う「分割片」をユーザサイドに渡し、対になる「分割片」をシステムで管理することで、毎回異なる「分割片」の組み合わせによるログイン認証を行うことができる。すなわち、一種のワンタイムパスワードとして活用することが可能である。

(4) DRM

秘密分散を行う時に付帯情報を添付できるようなシステムを構築した場合、秘密分散したものは元

と同じ価値を持たないことを利用して、著作物に著作権という付帯情報を添付し、かつ著作物ではない、という状況を作り出すことができる。これは一種の DRM の技術と考えることができる。

例えば、著作物等をオンライン表示しユーザサイドにデータを残さないようなケース=違法コピーを防止するような運用においては、ネットワークの性能により使い勝手が非常に悪くなることがある。ユーザサイドに大きな「分割片」、管理サーバ側に小さな「分割片」を配置し、オンライン表示時は小さな「分割片」データのダウンロードだけで済むような仕掛けを提供可能である。

［活用例］

- ユーザごと・著作物ごとにことなる秘密分散を行い、かつ「分割片」の分散管理を行うことで、著作物の不正なコピーを完全に防止することができる可能性がある。

[応用例]

- それぞれ異なる「分割片」をチケットのような感覚でクライアントに配布し、サーバで対となる「分割片」と組み合わせて原本情報を確認する。この場合、権利情報を原本とすることで、認証されたチケットとして活用することができる。
- 同様に、サーバで統合・復元し確認する時に、回数情報を管理することで、回数情報付きチケット=回数券として活用することが可能となる。
- オンラインの場合、ネットワークが繋がっていないケースもありうる。IC カード等に「分割片」を入れることで、ネットワークに繋がっていなくても DRM が実現できる可能性がある。（IC カード等がコピーできないことが条件）

8. 代表的な秘密分散技術について

最後に、現時点で手に入れることができる代表的な秘密分散技術について簡単に紹介しておく。

まず、最も採用数が多いと考えられるのは閾値秘密分散法だと思われる。これは数学理論でもあり、また「分割片」の一部をそろえて「原本の複製」を作成する方式の実現が簡単であることを考えれば妥当であろう。もちろん、閾値秘密分散法にもいくつかの方式があり、様々な企業が独自の実装を行っているので、各企業が公開している情報を確認されたい。

閾値秘密分散法ではない独自方式を採用している企業としては、本タスクフォースのメンバーでもあるグローバルフレンドシップ社をあげておく。こちらも、方式については当該企業が公開している情報を確認されたい。

以上

次世代電子商取引推進協議会
情報セキュリティ WG（TF1）　　御中

情報分散管理技術（電子割符技術を利用した情報管理）に関する法的意見書

2010 年 2 月 1 日
牧野総合法律事務所弁護士法人
弁護士　牧野　二郎

この度、次世代電子商取引推進協議会情報セキュリティ WG よりご依頼いただきました電子割符技術を利用した情報管理に関する法的意見をまとめましたので、以下の通りご報告申し上げます。

記

はじめに

今般、個人情報の漏えい事件が多発し、その規模も再び大型のものとなりつつあり、情報管理に関して憂慮すべきものと指摘されているところである。これまで各企業において情報の管理強化を実施してきた結果、端末からの漏えいは大幅に減少した。しかし、その対策の結果、情報の一元管理が進み、また、サーバへの情報の集中が進んだ結果、大量の情報を管理・利用する権限を持つ管理職、専門職が増加することとなった。

こうした管理職、専門職の階層においては、情報の活用が強く求められ、それに伴い比較的大きな裁量が与えられた。管理職、専門職に付与された裁量の範囲内での情報処理はその担当者の権限と責任に委ねられることが多い。

こうした背景があり、管理職のミスや背信行為が原因となる情報漏えい、大量の個人情報の外部流出といった事故が発生する結果となった。

従業者の端末からの漏えいは小規模のものに抑えられてはいるものの、管理職の大量漏えいの危険は、益々増加しているというのが現実である。

現在、こうした新しい危険に対する対応策が強く求められている状況にある。こうした環境おいて、電子割符の有効性、関連法規における位置づけ、法的評価が必要となった。

そこで、本意見書では、電子割符の技術の調査検討の結果を踏まえて、以下の通り法的見解をまとめた。

第 1　技術と運用に関する基本的視点

1　前提となる視点

本来法的評価、法的意見書の作成は、①提供されている技術そのものの検討・評価、さ

らに②その技術を運用する運用者側の運用ルールや、運用実態、リスク分析などを踏まえた運用の評価、更に③以上二つの対象の検討・評価を踏まえて、総合的な視点から、実用的運用における法的評価、法的責任（善管注意義務に関する評価）を検討すべきである。

本意見書は、上記①は電子割符技術が確立していることから、その概要を把握して評価すること、及び②は実用を評価対象とするものではないため、問題点の指摘にとどめ、今後の電子割符技術の活用促進に資する問題点を指摘し、更に③については、電子割符技術を、ビジネスに提供することで、得られる安全性を中心に検討し、その際の法的課題を明確にすることに主眼をおいた。

本件の検討対象となる電子割符技術は、管理行為とは区分された技術的成果として確立している。電子割符技術は、秘密分散技術の一つとして、特許申請がなされているものでもある（特開 2004-053969 電子割符生成方法およびプログラム 他申請　参照)。

どのような高度な技術の提供であっても、それを運用する側の運用がずさんであれば技術の優位性を発揮すること自体が困難となる。又、反対に、技術が余りに難解であれば、その難解さゆえに、運用者がその技術を理解できず、その結果合理的運用が確保されないという状況の原因ともなる。

本件電子割符技術は、かつての我が国と中国との勘合貿易により確立された認証証明技術をヒントとして、それをデジタルデータ処理に生かしたものとも言われており、歴史的背景に照らしても実用的かつ簡易な手法であり、運用者には理解しやすい技術として構築されている。

本件は、情報セキュリティ、情報保護、個人情報保護などを基本的な目的としていることから、法的要請に答えるためにもその範囲の関係法規を検討し、その違反事例を念頭に、本件技術を検討し、更にあるべき管理体制などについても検討することとする。

第２　前提となる法的枠組み

これまで情報セキュリティに関する法制度は必ずしも明確にされていなかったが、会社法の制定（平成 17 年商法改正）により、情報セキュリティ対策のための制度整備の義務が企業の内部統制システム構築義務の、具体的内容の一部として盛り込まれた。

また、個別の業務規制法として、例えば個人情報保護法（平成 15 年 5 月制定)、不正競争防止法などにおいても情報セキュリティの法的根拠が与えられており、情報管理、情報セキュリティの強化は、全ての企業にとって必須のものとなり、情報管理体制整備の確立に十分な対応をしていない場合には、全ての経営管理者（会社役員）に法的責任が課されるなど、厳しい制度となっている。

その概要は、以下のとおりである。

法的責任の概要

（1）会社法第 362 条（取締役会の権限と責任）4 項 6 号

法令定款適合性及び業務適正性確保のための体制整備義務

会社法施行規則

100 条 1 項 1 号　職務上記録の保存

同条同項 2 号　　損失に危険管理のための体制整備義務

（2）個人情報保護法

20 条（安全管理措置義務）及び 21 条（従業者監督義務）

個人情報漏えい防止のための必要かつ適切な措置を実施する義務

（3）著作権法コンテンツ管理

権利者からの許諾を遵守するためにコンテンツ管理を行う義務がある。

実効性のあるコンテンツ管理は、契約責任で明確にされる。

その基礎には法の権利規定（17 条以下、21 条複製権など）に基づく、許諾行為がある。

（4）不正競争防止法

「営業秘密」として保護されるためには、秘密として管理されていることが必要とされ（第 2 条 6 項）、秘密として管理されていない情報は不正競争防止法による法的保護を受けないものとされている。

（5）その他　銀行業法、保険業法、証券取引法など、多数

これらの法的制度整備に伴い、法的責任が明確になってきており、企業の情報管理においては法的責任を果たすためにも、より簡易で、合理的な情報管理の方法が求められている。

電子割符技術は、その中の重要な技術として提案された。

第 3　実例に見る情報管理の困難さ

個人情報の漏えい事故においては、安全管理措置義務違等を理由として、監督官庁が事業者に対して業務是正勧告を行う事例が多数出ている。中でも、以下のような重大な事案を検討する必要がある。

①2004 年 4 月　株式会社みちのく銀行における個人情報漏えい事件

当該銀行の顧客情報が約 128 万件（うち個人情報約 124 万件）の記録された CD3 枚を本支店間の情報移動の際に紛失してしまった事案。情報移動の際の安全を確保する体制整備ができていないため行政指導を受けることとなった。

②2006 年　みずほ銀行における個人情報漏えい事件

幹部社員の課長時代の名簿販売が後に発覚、逮捕時監査部調査役になっていた事案。持ち出した情報は 628 名分であったが、銀行はこれを事前・事後に発見できず、個人情報が外部に漏れているという警察からの問い合わせによって始めて発覚するという事態であることが重視され、銀行の管理体制が問題とされた。銀行法上の業務改善命令に加えて、個人情報保護法上の勧告がなされた。当該行員は、業務上横領容疑で逮捕された。

③三菱 UFJ 証券個人情報漏えい事件

この事件は、システム部元社員が、顧客情報約 150 万件を不正に取得し、さらにこのうち約 5 万名分のデータを名簿業者へ売却した事件。発覚後、情報の回収を進め、被害を防止したものの、大量のデータを安易に引き出し、自宅へ持ち帰ることができた点で重大な問題を提起した。

④2010 年 1 月　あらた監査法人個人情報漏えい事件

監査法人の社員が、顧客情報が格納されたノート PC を持ち歩いていたところ、盗難に遭い、個人情報を漏洩したが、ノート PC には暗号化などのセキュリティ対策を実施していたため、現実的リスクは無いと説明されている。

ただし、当該セキュリティ対策が破られ、あるいは簡易なパスワードなどであった場合には、簡単に解読、復号化される危険性は否定できない。

以上の具体的事例の検討からも明らかなことは、個人情報の漏えいは未だ頻繁に発生しており、その原因の多くは、既に指摘されてきた安全管理措置が不十分であり、また、管理者の行為が管理されず、無断流出が管理されていない、といったものであり、これまでの対策や制度整備では十分な対応は困難であることが示されている点である。

事件事故を発生させてしまった企業は、いずれもセキュリティ対策について対応をしてきたことが確認されており、漫然と放置していたわけではない。企業に求められる一般的対策を実施していたにもかかわらず、発生してしまったとの報告がほとんどである。これは、対策の多くが個人の注意や努力に依存し、あるいは管理に委ねられるという実態があることから、個人の注意力低下や、管理点検ミスにより、いつでも現実化するリスクを抱えていることを示している。

従って、個人の努力のみに依存せず、体制として、システムとして機能するセキュリティ技術、及びその技術が十分に活用されるための管理手法、マネジメントが強く求められる。

第 4　電子割符の特徴と法的安全性について

この度、次世代電子商取引推進協議会情報セキュリティ WG におかれては、電子割符の技術の検討を行い、今後の普及を目指して、情報管理技術としての分析評価を行っている。同技術は、政府の推進するセキュリティ対策に関する施策の中で取り上げられているものであるが、情報漏えい対策に有効な技術として更に活用が求められているとの認識がなさ

れている。

（1）電子割符の特徴

元になる個人情報自体を、科学的技術を利用して複数の割符に非線形に分割し、保管、移動に安全な環境を与え、後にそれらが全て集合した場合に復元可能とした技術である。

電子割符技術は、元のデータを分割して生成した電子割符のうち、どれか一つでも欠いた場合には統合・復元できない特性を持つデータ群を構成する。

この技術では、データの統合・復元の権限を留保するためには、割符のいずれかの一片をデータ管理者のみ保有することで、統合・復元を阻止できる。すなわち、割符所有者全員の同意がない限り統合・復元できない、ということによる安全性を実装した。

また、一つの元データを複数の割符に分割する際も、割符構成のための分割の都度、生成される割符情報のそれぞれが異なるデータ内容となるため、別の機会に作成した他のデータとは統合・複合ができない仕組みとなっている。

このことから、割符の統合・復元に特定の鍵を必要としないため、鍵の保有者のみが統合・復元の権限を留保する仕組みとは異なる。

個人情報などの移動のために、割符を持ち出したがこれを紛失、盗難により、一部外部に漏えいする事態が発生した場合も、不正取得者が、元の情報へ復元しようとしても、統合、復元ができないため、安全性を確保できるとされる。

（2）電子割符の優位点

電子割符の一部の取得だけでは、元データの復元は不可能であり、仮に、解析を成功させたとしても、他のデータ部分が含まれてはいないため、結局、全てのデータを取得しない限り、元のデータへの復元を実施できないという優位点がある。

従って、文書、各種データを保有・管理する権限者は、当該電子割符の仕組みを利用して、復元不能な電子割符を作成し、安全性を確保するという。

（3）従来型暗号システム（電子署名を含む）との比較検討

現在政府を始め、情報の暗号化の仕組みとして利用されている電子署名制度は、管理者が予め作成し、保有する鍵（公開鍵とペアとなる秘密鍵）を利用して、暗号化と複号化を実施するものである。

この鍵は、鍵生成後、相当長期間（1 年乃至 3 年前後）にわたって利用されるものとなっており、その間に解読されてしまえば、内容を復元・復号化することが可能となる。

現在政府では、現行の暗号方式である SHA1 方式は、既に危険性が指摘されたとして、新しい方式への移行手続きが進められている。

このように公開鍵暗号方式は現在政府も利用している高度な犯罪対策の一つではあるものの、暗号解読の危険が予想されることから、常に高度な暗号アルゴリズムへの変更

が求められる。

その結果、利用者は、その都度新しい暗号に対応するため、新しい鍵の発行を受けると共に、新しいシステムに対応したプログラムとするなど、コストと手間を必要とする対応が求められる結果となる。

これに対して、電子割符は、分け方に典型的なルールがないことから、暗号などの「鍵」が存在しない分、利用者には利用しやすいものといえる。鍵が存在しないということは、鍵の管理から開放されることを意味しており、法的責任の基礎となる善管注意義務についても、そのレベルを低減する効果を持つ。利用者は困難な管理から開放され、簡易な管理方法によっても注意義務が果たせるため、リソースを他の部分に回せるというメリットがあると評価できる。

(4) 運用管理面での特徴と今後の課題

① バックアップデータの保管管理

ただし、電子割符の一片でも紛失した場合には、統合・復元が不能となることから、運営管理上は、元データのバックアップの必要が出てくる。万が一、電子割符の一部が紛失、盗難となった場合には、残るデータは無意味な情報となることから、それに代わる新しいデータを生成が必要となる。

② 利用場面での電子割符の統合・復元との関係

個人情報を利用し、活用する日常的場面においては、電子割符となり、分割されたデータを頻繁に、統合・復元する必要が出てくるため、そのための作業が課題となる。利用者にとって簡易かつ迅速で、しかも電子割符の有効性を損なわない統合・復元システムが実装される必要がある。

第 5　電子割符と個人情報

(1) 非個人情報としての電子割符の評価

従来から、個人情報に対して暗号による保護措置を実施した場合に生成される暗号化された個人情報データは、仮に復号化が困難で、暗号文の状態では自然人に読めない場合であっても、なお、個人情報であるとされる（経済産業省ガイドライン)。これは、暗号化した情報であっても、暗号化した情報自体がオリジナルデータの全てを含有しており、復号のための鍵が存在する場合には、容易にオリジナルデータが復元できてしまうことに由来している。現実にも、暗号化した際に、複合するための鍵を別媒体に保管して、別異に管理していれば良いが、同じ PC、モバイル内に蔵置する場合には暗号化の意味は大きく減殺される結果となることが指摘されている。

これに対して、電子割符の場合は情報を非線形的に分割し、オリジナルデータ自体を分離、分割してしまうことから、分割後の割符それぞれには全情報が含まれておらず、

単体としては不完全な情報となる。この結果、電子割符は個人を識別する情報を持たないことになり、暗号化された情報とは異なる評価が与えられることになる。
個人情報保護法上の「個人情報」であるためには、当該情報から個人が識別され、あるいは暗号などであっても、ある種の措置により復元可能である場合にはなお個人情報となるとされるが、この要件からは電子割符を評価すれば、単体としての電子割符の情報は、（他の割符と容易に照合ないし結合できる状態でない限り）個人情報とはいえない情報であるということができる。

(2) 管理手法における復元の危険性について

以上電子割符が、単体では個人情報とはいえない情報であるとしても、管理において十分な対策がなされていない場合には、なお、統合・復元の危険性が存在することも指摘されなければならない。

単体の電子割符の情報から元の個人情報は復元できず、また、復元のための復号鍵はないため容易には復号化できないとしても、仮に、全ての割符がそろい、統合・複合化のためのプログラムが提供される環境にあっては、特段の困難性なく、統合・復元が可能であると考えられる。この事実からは、取扱事業者の手元にある場合はもとより、分散され別異に管理されていても、究極的に同事業者による統合が可能な場合には、なお統合・復元は可能であると評価されることになる。

電子割符は、技術的評価として個人情報とはいえないデータ群を生成するものといえるが、その技術を十分に管理せず、運用のレベルにおいて統合・複合可能とすることが可能であることから、管理手法の確立と環境の整備が同時に行われることが必須となる。

従って、事業者は電子割符の技術を利用して、個人情報を分割し、安全な情報とすることを前提とした上で、更に個人情報保護法に従って、全ての電子割符を適正・安全に管理すべき法的義務を負うことになる。

その結果、管理ミスによるなどして、電子割符が一つでも目的外、想定外に流出した場合には、なお、個人情報保護法違反と評価される危険の存在を認識しなければならない。すなわち、電子割符は、事業者の管理責任を免れさせる技術ではなく、あくまで漏えい時の損害を防ぐ、または減少させるための技術であると位置づける必要がある。

この管理義務は、電子割符が、同一事業者の利用に供され、その実質的管理下にある場合に認められる他、個々の電子割符を移送し、交付、発信する場合にも、移動中に管理下から離れないように、安全管理措置を施すべきことが求められることになる。従って、情報の移送中についても、十分な注意義務が果たされる必要がある。

(3) 電子割符の管理が移転する場合

既に指摘したように個々の割符データ自体は個人情報そのものではなく、個人情報が分割された後の、何分の一かの部分でしかないため、単体での復元は不可能であることから、単体としての電子割符を持つ事業者にとっては、それはもはや個人情報というこ

とはできない。

従って、容易に統合・復元できる環境で、同一の事業者、管理者が全ての電子割符を管理している場合には、未だ個人情報ではあるものの、それらの個々の電子割符が、元の事業者のもとに残らず異なる事業者、受領者の下に移転し、管理されるに至った場合には、それら移転後の個々の電子割符は、もはや個人情報ではなく、受領した事業者においては個人情報保護法の適用がなく、個人情報取扱事業者としての法的義務も負担するには至らないと考えられる。

以上から、個々の電子割符自体は、個人情報ではないと考えられるため、その情報を受領した者は、対象情報を個人情報として取り扱う義務までは負うことなく、通常の取引における情報と同程度の情報として取り扱うことも可能となる。

個人情報取扱事業者が電子割符技術を利用して作成した個々の電子割符を、移動に際して暗号化するなど、安全な措置を採用した後、これを移送事業者に移送を委託し、あるいは電子メールなどによる伝送、各種記憶メディアに記録した場合、これらの個々のデータは個人情報とは言えないため、受領者において特段の法的義務を負うことにはならない。

その結果、関連事業者にあっては、安全対策などは格段に低減され、管理の負担を軽減することが可能となる。

第６　法的リスクの低減効果

一般に、個人情報の漏えいの場合、漏えい事故を起こした企業は様々なリスクを負担することになる。漏えいした事実を公表し、謝罪し、信用を保護すべく多大なコストと作業が必要とされ、また、漏えいした情報の本人が原告となり、訴訟を提起される危険も存在する。

こうした社会的、経済的リスク及び訴訟リスクを回避する点で、電子割符は有効に機能すると考えられる。

(1) 経済的損失の回避

すなわち、電子割符が、個人情報を非線形的に分割して、一つ一つの電子割符自体が個人情報の部分としてのデータでしかないものとしていることから、そのデータだけでは、割符一つのみを持つ事業者にとっては個人情報としての意味を持たないとされる。

その結果、仮に個々の電子割符が漏えいしたとしても、それを受領した者は、それが個人情報であるか、その断片であること自体を理解することはできないとされ、そうであれば、情報本人の識別情報や属性情報が悪用される（負債情報を元に振り込め詐欺などが行われる危険など）ことはなく、被害は発生しない。

(2) 訴訟リスクの回避

一般に訴訟を提起する場合、原告となろうとする者が、自らの権利を侵害するものであることを示す必要がある（原告適格）。ところが、本件における個々の電子割符の場合、その情報からは識別情報の復元は可能ではないとされ、当該電子割符が誰の情報であるかを特定することができず、結局仮に誰かがこれを取得したとしても、その情報が自身のもの(個人情報)であることを立証することができないため、原告たり得ないという結論となる。

こうして、電子割符技術により、多くの場合訴訟リスクも回避されると考えられる。

ただし、全ての電子割符が事業者の手元に存在する場合、また、それを管理するという関係からは統合・復元が可能である限りにおいて、既に述べたように当該事業者にとって、それらの情報は未だ個人情報であるため、その一部分でも漏えいする場合には、個人情報の一部の漏えいと理解される危険がある。その点で個人情報の管理において、管理ミスがあったと評価されるため、内部統制上は、個人情報の管理体制の確立、充実に向けて厳しく対応しなければならないこととなる。

第7　まとめ

電子割符の技術は、情報セキュリティ対策において、情報の分割を前提とすることから、オリジナルデータの分割後の単体としての電子割符からもとのオリジナルデータが復元できないという特性があり、その特性は情報管理技術として高く評価されるものである。

個人情報保護法の視点からも、それら単体の電子割符のデータは個人情報とはいえない情報となるため、分散管理のコストや移送における管理コストの削減などに大きく寄与するといえる。

電子割符の技術は、こうして法的観点からも、情報管理体制整備を進める上で、有効な技術と評価することができる。

しかし、同時に、電子割符は技術として提供されるため、それを管理する管理手法の整備が伴わなければならないことは言うまでもない。いくら優秀な技術であっても、運用のルールや運用における点検整備が実施されない限りは万全のものとはならない。

情報管理の主体となる企業は、当該電子割符技術を導入して、情報の分割による技術的安全対策を実施すると共に、分割後の電子割符を安全に管理、統制するための組織的、人的管理を進める必要がある（経済産業省個人情報保護ガイドライン参照）。

また、当該電子割符技術が広く普及、活用されるためにはこうした管理手法や管理制度に対する簡便なガイドラインの提供、ソフトウエアによる運用支援が行われることが有効であり、更なる発展を期待するものである。

以上

EC における情報セキュリティに関する活動報告書 2009

平成 22 年 3 月　発行

発　行　　次世代電子商取引推進協議会

販　売　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園 3 丁目 5 番 8 号
機械振興会館 3 階
TEL:03（3436）7500

この資料は再生紙を使用しています。