情報セキュリティにおける失敗事例とその類型化に関する一考察

佐藤 亮太† 高橋 克巳† 桑名 栄二†

†NTT 情報流通プラットフォーム研究所
185-8585 東京都武蔵野市緑町 3-9-11
sato.ryota@lab.ntt.co.jp takahashi.katsumi@lab.ntt.co.jp kuwana.eiji@lab.ntt.co.jp

あらまし 企業や大学などの組織における情報セキュリティの事件や事故が多発し，それらいわゆる失敗に対するマネジメントが，その組織の事業継続にとって重要となっている．一方で，機械工学の分野では，各失敗事例から，その失敗知識を抽出することで失敗を次へ活かす失敗学が発展している．そこでは，失敗事例をその原因に基づき類型化し，失敗マネジメントの出発点とする研究が存在する．本稿では，組織において実際に発生した情報セキュリティの失敗事例を収集し，それらの原因を分析する．さらに，その原因について，既存の類型化を参考としながら，情報セキュリティ分野における類型化を試みる．

A Study of Failures of Information Security and Its Classification

Ryota Sato† Katsumi Takahashi† Eiji Kuwana†

†NTT Information Sharing Platform Laboratories
3-9-11, Midori-Cho, Musashino-shi, Tokyo, 180-8585, JAPAN
sato.ryota@lab.ntt.co.jp takahashi.katsumi@lab.ntt.co.jp kuwana.eiji@lab.ntt.co.jp

Abstract Recently a lot of information security incidents or accidents have occurred then it has been more important for organizations to manage these failures. On the other hand, the study of failure which focuses on the knowledge of failures to apply it to other failures has been developed in mechanical engineering. There is an approach which classifies the failures based on its causes to derive the knowledge in the study of failures. In this paper, we collect the cases of the failures in information security and try to classify them based on its causes.

1 はじめに

多くの企業や大学などの組織において，不正アクセスによる大規模な個人情報の漏洩事件や従業員による電子機器の紛失に伴う機密情報の漏洩事故など，情報セキュリティにまつわる事件や事故は後を絶たない．これら事件や事故といった，いわゆる，組織の情報セキュリティの失敗に対する適切なマネジメントが，その組織の事業継続にとって重要な課題となっている．

一方で，各組織においては，組織の情報セキュリティを管理するため，ISMS（Information Security Management System）の構築などの対応が取られている[1]．ISMS は，自らのリスクアセスメントにより必要なセキュリティレベルを決め，プランを持ち，資源配分して，システムを

運用するための仕組みである.

また, 発生した失敗に対応するための計画や管理の仕組みとして, BCP（Business Continuity Plan）や BCM（Business Continuity Management）がある. BCP では, 事故や災害などが発生した際に,「いかに事業を継続させるか」もしくは「いかに事業を目標として設定した時間内に再開させるか」について様々な観点から対策を講じるための計画であり, BCM は, BCP の策定から運用, 見直しを含むマネジメントである[2].

これら失敗に対するマネジメントシステムは, 個々の組織において構築される. したがって, これまでに発生した様々な情報セキュリティの失敗は, 発生した組織内においては, そこから得られた教訓や知見が管理され, 次の組織活動へと活かされてきた. これらの教訓や知見を, 組織の枠を超えて共有することができれば, 各組織の情報セキュリティ対策にとって非常に有用である. そのためには, 一般的に, 組織内で機密情報として管理される, 情報セキュリティの失敗事例を収集, 分析し, それらを共有できるような形で知識化する必要がある.

本稿では, 実際に発生した情報セキュリティの失敗事例を収集し, それらの原因を分析する. さらに, 失敗事例の知識化に向けて, 機械工学の分野で発達している失敗学の考え方を参考としながら, 分析した原因の類型化を試みる.

2 関連研究

組織における失敗マネジメントに対する考え方の一つとして, 失敗学が, 主に機械工学の分野で発達している[3]. 失敗学においては, 例えば, 橋の崩落事故や船の沈没事故, 飛行機の墜落事故などの失敗を研究対象としている. また, 失敗を「人間が関わって行うひとつの行為が, はじめに定めた目的を達成できないこと」と定義した上で, 様々な失敗事例の原因分析を通じて, 失敗原因の階層構造や失敗情報の伝達時の特徴などをまとめている. そして, 発生した失敗を罰するのではなく, 許容し, その失敗を忘れるのではなく, 次へと伝え, 活かしていくことが重要としている. つまり, 個々の失敗事例から共通した課題を抽出し, 抽象化した失敗知識を, 次の新たな組織活動へ展開することで, 新たな失敗の未然防止が可能とされている.

その失敗知識の具体例として, 失敗事例に共通した原因を類型化した先行研究が存在する[4][5]. そこでは, 機械工学の分野における失敗事例を約 200 件収集し, それらに共通の原因を抽出している. その結果, 表 1に示す, 41 分類に類型化できるとしている.

表 1 機械工学における失敗原因の類型化

大分類	中分類	小分類
1.技術的な要因で, しかも機械分野のエンジニアが少なくとも最初に考えるべき力学的な設計要因	1.材料の破壊	1.脆性破壊, 2.疲労破壊, 3.腐食, 4.応力腐食割れ, 5.高分子材料
	2.構造の破壊	6.バランス不良, 7.基礎不良, 8.座屈
	3.構造の振動	9.共振, 10.流体振動, 11.キャビテーション
	4.想定外の外力	12.衝撃, 13.強風, 14.異常摩擦
2.技術的な要因だが, 普通は副次的に考えている使用時の設計要因	5.想定外の制約	15.特殊使用, 16.落下物・付着物, 17.逆流, 18.塵埃・動物, 19.誤差蓄積
	6.火災・天災からの逃げ遅れ	20.油脂引火, 21.火災非難, 22.天災非難,
	7.連鎖反応で拡大	23.脆弱構造, 24.フィードバック系暴走, 25.化学反応暴走, 26.細菌繁殖, 27.産業連関
	8.冗長系の非動作	28.フェイルセーフ不良, 29.待機系不良
3.技術的な要因だが, 人間や組織との関係が強い設計要因	9.作業で手を抜く	30.入力ミス, 31.配線作業ミス, 32.配管作業ミス
	10.設計で気を抜く	33.自動制御ミス, 34.流用設計, 35.だまし運転
4.技術ではどうしようもない組織的な要因	11.個人や組織の怠慢	36.コミュニケーション不足, 37.安全装置解除
	12.悪意の産物	38.違法行為, 39.企画変更の不作為, 40.倫理問題, 41.テロ

また, プログラミング知識の学習環境の構築にあたって, 失敗学の考え方の適用も検討されている[6]. そこでは, プログラミング知識の定着にとって, 学習者が学習中に起こした失敗を自ら内省する過程が重要であるとしている. そして, 失敗が発生した際に, 失敗学で定義されている失敗知識のもつ属性に沿ってその失敗を記録させ, 学習者の内省を促進する環境の提案と実装をしている. また, その実装を用いた実験では, その環境による学習効果の向上が確認されている.

失敗マネジメント以外に, 情報セキュリティの失敗事例に関する統計的な調査も存在する. 特に, 個人情報漏洩に対しては, 新聞やインターネットニュースなどで報道された事例に対する継続的な調査がされている[7]. ここでは, 漏洩の原因を「設定ミス」,「誤操作」,「バグ・セキュリ

ティホール」,「不正アクセス」,「内部犯罪・内部不正行為」,「不正な情報持ち出し」,「目的外使用」,「紛失・置忘れ」,「盗難」,「管理ミス」,「ワーム・ウィルス」,「その他」,「不明」の 13 個で定義し, 原因ごとの発生頻度などを提示している.

3 情報セキュリティ失敗事例

我々は, 約 1.5 年間の間に, 複数の組織において, 実際に発生した情報セキュリティの失敗事例を 41 件収集した. これは, 実際に被害が発生した事例だけでなく, 被害を未然防止できた事例も含んでいる. 本章では, そのうち 3 件を, 概要, 原因, 結果, 対処に分けて示す. また, 概要は, その失敗事例の経過が分かるよう表示した. さらに, 結果は, 機密性, 完全性, 可用性の観点から, 対処は, 予防, 抑止, 検知, 回復の観点からまとめている.

3.1 顧客端末へのウィルス感染拡大

○概要
[n 日午前] A 社へ, 顧客である B 社から, A 社提供のサービスの遅延に関する問合せあり. B 社のネットワークに接続された A 社内 PC から通信状況を調査し, n-1 日の夕方から異常なトラフィックの上昇を確認.
[n 日昼] A 社内 PC のウィルス対策ソフトの定義ファイルを最新化し, ウィルススキャンを実施したところ Conficker ワームを検出. A 社内 PC をネットワークから切断し, 当該ワームに関する調査を開始.
[n+4 日] A 社から B 社への調査状況の報告を実施. A 社内 PC への計画作業で利用した, 個人の USB 媒体経由での感染の可能性が高いことを報告.
[n 日+1 ヵ月] 感染経路等の調査に 1 ヵ月を要した. USB 媒体への感染元 PC を特定するも, 当該 PC が感染した理由は不明.
[以降, 経過情報なし]
○原因
マルウェア, 最新定義ファイルの未設定, 個人 USB 媒体の不正利用.
○結果
機密情報漏洩の可能性(機密性), A 社 PC をネットワークから切断することで事業継続が困難(可用性)
○対処
ウィルス活動に必要なパケットに対するフィルタリング設定(予防), 最新定義ファイル更新の頻度向上(検知), 感染 PC のリアルタイム監視システムの構築(検知)

3.2 Winny 経由での機密情報漏洩

○概要
[n 日] A 社の業務委託先である C 社の従業員が, 自身の個人端末に A 社機密情報を入れた状態で, Winny を利用. Antinny 系ウィルスに感染し, A 社機密情報が流出.
[n+11 日] A 社機密情報が Winny 上で流出していることを, D 社が発見.
[n+12 日] D 社から A 社へ流出を通知. A 社にて, 流出した情報の種類や総数を確認.
[n+15 日] A 社内でエスカレーション後, 経営者会議にて, モニタリング継続との対応を決定.
[n 日+1 ヵ月] 某掲示板サイトにて, A 社機密情報の投稿を予告する書き込みが発生.
[n 日+5 ヵ月] C 社従業員の感染 PC のデスクトップ画像が Winny 上で流出していることを確認.
[以降, 経過情報なし]
○原因
マルウェア, 業務委託先によるルール違反, 業務委託先の管理不徹底.
○結果
機密情報の漏洩(機密性), 信用失墜により事業継続が困難(可用性)
○対処
情報管理ルールの再確認(予防), 業務委託先の管理徹底(抑止)

3.3 Web サイトのコーディングミス

○概要
[n 日] A 社の社外向け Web サイトの画像認証

表 2 脅威と脆弱性の例

<table>
<tr><th colspan="2">人為的脅威の例</th><th rowspan="2">環境的脅威の例</th></tr>
<tr><th>意図的脅威</th><th>偶発的脅威</th></tr>
<tr><td>故意の損害，盗難，記憶媒体の不正使用，ユーザIDの偽り，違法なソフトウェアの輸入/輸出，不正なユーザによるNWへのアクセス，不正な方法でのNW設備の使用，盗聴，通信への侵入，トラフィック分析，メッセージ経路変更，否認</td><td>停電，断水，ハードウェアの故障，NW構成要素の技術的障害，送信エラー，メッセージ経路選択の誤り，スタッフ不足</td><td>地震，台風，落雷，ほこり，静電荷，記憶媒体の劣化</td></tr>
<tr><td colspan="2">争議行動，爆破行動，武器の使用，火事，空調故障，操作員のエラー，保守のエラー，ソフトウェアの故障，不正なユーザによるソフトウェアの使用，不正な方法でのソフトウェアの使用，ソフトウェアの違法な使用，悪意あるソフトウェア，回線の損傷，トラフィックの通負荷，通信サービス（NWサービス）の障害，ユーザのエラー資源の誤用</td><td></td></tr>
<tr><td colspan="2">電力の不安定</td><td></td></tr>
<tr><td colspan="3">洪水，極端な温度および湿度，電磁波放射，操作員のエラー，保守のエラー，ソフトウェアの故障，不正なユーザによるソフトウェアの使用，不正な方法でのソフトウェアの使用，ソフトウェアの違法な使用，悪意あるソフトウェア，回線の損傷</td></tr>
</table>

脆弱性の分類	脆弱性の例
ソフトウェア	監査証跡の欠如，不十分なパスワード管理，アクセス権の誤った割り当て，管理されていないソフトウェアのダウンロード， ワークステーションから離れる際に“ログアウト”しない，文書化の欠如
ハードウェア	記憶媒体の不十分な保守/不適当な設置，有効な構成変更管理の欠如， 記録媒体の定期的な交換計画の欠如
通信	保護されていない通信回路，送信元および受信社の識別と認証の欠如， 平文でのパスワード転送
文書	保護されていない保管，廃棄時の注意欠如，管理されていないコピー作成
人事	要員の不在，不十分なセキュリティ訓練，セキュリティ意識の欠如， ソフトウェアおよびハードウェアの正しくない使用，不適切な採用手続き
環境，施設	建物，ドアおよび窓の物理的保護の欠如，建物，部屋への物理的アクセス管理の不適当または不注意な使用，洪水の影響を受けやすい地域への配置

(CAPTCHA)の文字列が，HTML ソースの表示から確認できることを，A 社社員が発見.
[n+5 日] コーディングミスを修正し，Web サイトを再リリース.
[以降，経過情報なし]
○原因
コーディングミス
○結果
利用可能な認証 ID 一覧の漏洩の可能性(機密性)，修正中に Web サイトが利用不能(可用性)
○対処
コーディング技術の向上(予防)，サービスリリース前の試験手順の見直し(予防)

4 失敗原因の類型化

前章では，情報セキュリティにおける失敗事例について記載した．本章では，それら原因の類型化を通じて，失敗事例の知識化を試みる.

4.1 類型化の目的

前述の通り，失敗事例は組織内で機密情報として管理される場合が多く，他組織へ展開され難い．また，失敗事例は，それが発生した組織固有の環境下での事例である．そのため，多くの失敗事例をそのまま他組織へと展開しても，類似点に気付くことができず，有用な情報として活用されない可能性がある[5]．そこで，複数の失敗事例に含まれる前提や原因，結果といった要素から，他組織の事例へも演繹可能な類似点を抽出する，類型化が有効となる．特に，表 1のような，原因に基づく類型化の各項目に，過去の失敗事例やその対策が対応付けられれば，他組織においても普遍的な失敗知識として活用が得られると考えられる.

4.2 類型化の方針

表 1に示す，機械工学における類型化を，情報セキュリティ失敗事例の原因の類型化に向けた出発点とする．組織的な要因が関係する項目，つまり，大分類3，4は，情報セキュリティにおいても共通的に利用できる可能性が高いと考えられる．一方，技術的な要因が関係する項目，つまり，大分類1，2は，適宜変更する必要がある.

また，表 1と情報セキュリティでは，失敗の原因に対する考え方に差異があり，注意が必要である．情報セキュリティにおけるリスク因子には，表 2に例示する，脅威と脆弱性がある[8]．脅威は，「システム又は組織に損害を与える可能性があるインシデントの潜在的な原因」，脆弱性は，「一つ以上の脅威がつけ込むことのできる，資産又は資産グループがもつ弱点」と JIS Q 13335-1：2006 において定義されている．そして，情報セキュリティのリスクは，脅威と脆弱性が組み合わさった結果，失敗事例として健在化すると考えられている．一方で，表 1では，脅威と脆弱性の考え方が明確に反映されていない．これは，機械工学の分野では，情報セキュリティの分野とは異なり，組織外の人が脅威源となる失敗が少ないためである．例えば，橋の崩落事故における脅威は，風など橋への振動を引き起こす自然現象が主であり，環境的脅威に分類さ

表 3 既存の類型化に対する脅威と脆弱性の例の対応付け

大分類	中分類	小分類
1.技術的な要因で，しかもシステム/ソフトウェアに関わるエンジニアが少なくとも最初に考えるべき情報セキュリティ的な設計要因	1.材料の破壊	1.脆性破壊，2.疲労破壊，3.腐食，4.応力腐食割れ，5.高分子材料
	2.構造の破壊	6.バランス不良，7.基礎不良，8.座屈
	3.構造の振動	9.共振，10.流体振動，11.キャビテーション
	4.想定外の外力	12.衝撃，13.強風，14.異常摩擦
	バグ・セキュリティホール	ソフトウェアの故障，NW構成要素の技術的障害
	内部関係者を利用しない攻撃	トラフィックの過負荷，トラフィック分析，メッセージ経路変更
	内部関係者を利用した攻撃	悪意のあるソフトウェア
2.技術的な要因だが，普通は副次的に考えている使用時の設計要因	5.想定外の制約	15.特殊使用(ユーザのエラーなど)，16.落下物・付着物，17.逆流，18.塵埃・動物，19.誤差蓄積，システム環境故障(停電，ハードウェアの故障など)
	6.火災・天災の影響	20.油脂引火，21.火災(火事)，22.天災(地震など)
	7.連鎖反応で拡大	23.脆弱構造，24.フィードバック系暴走，25.化学反応暴走，26.細菌繁殖，27.産業連関
	8.冗長系の非動作	28.フェイルセーフ不良，29.待機系不良
3.技術的な要因だが，人間や組織との関係が強い設計要因	9.作業で手を抜く	30.入力ミス(操作員のエラー)，31.保守作業ミス(保守のエラーなど)，32.配管作業ミス
	10.設計で気を抜く	33.自動制御ミス，34.流用設計，35.だまし運転，暗号や認証の欠如(保護されていない通信回線など)，物理的な保護の欠如(建物，ドアおよび窓の物理的保護の欠如)，記録の欠如(監査証跡の欠如など)
4.技術ではどうしようもない組織的な要因	11.個人や組織の怠慢	36.コミュニケーション不足，37.安全装置解除(離席時にログアウトしないなど)，不適切な情報管理(不十分なパスワード管理など)，不適切な要員管理(要員の不在など)
	12.悪意の産物	38.違法行為(盗難など)，39.企画変更の不作為，40.倫理問題(不正なユーザによるNWへのアクセスなど)，41.テロ(破壊行動など)

れる．したがって，既存の類型化を出発点とする際には，特に人為的脅威の観点も含め，必要に応じて，その項目を見直す必要がある．

4.3 脅威と脆弱性の例の対応付け

前節で述べた通り，情報セキュリティにおける脅威と脆弱性の観点を，表 1へ反映する．そこで，表 2に示す 68 個の脅威と脆弱性の例について，表 1の小分類の各項目へ対応付けを行った．なお，表 2の例は，ISO/IEC TR 13335：1997 が示した脅威と脆弱性の例として，参考文献[8]に記載されているものである．この対応付けにあたっての方針は下記の通りである．

- 大分類1，2には，脅威の主体が組織外となる人為的脅威を含める．
- 既存の大，中，小項目へ可能な限り対応付け，対応付け可能な例は，その小項目へ( )付けで記載する．
- 既存の項目では表現に変更が必要な場合や項目が不足している場合は，項目を修正，追加したうえで，例を対応付ける．

その結果を表 3に示す．ただし，複数の例が同一の項目へ対応づけられる場合，代表的な例を( )内に記載している．この結果，抽象度の大きな大，中分類レベルに対しては，技術的な要因を除いて，全ての脅威や脆弱性の例が対応付けされた．また，特に人や組織的な要因については，小分類レベルにおいても，多く項目が対応付け可能であった．

4.4 情報セキュリティ失敗事例の原因の対応付け

表 3に基づいて，第3章にて述べた事例を含む 41 件の失敗事例の原因の類型化を行う．このとき，1 つの失敗事例に対して，その原因は複数考えられる．本稿では，失敗事例 41 件から 55 個の原因を抽出した．これら 55 個の原因を，表 3へ対応付ける．対応付けの方針は前節と同様であり，( )内には対応付けられた原因の個数を記載する．

具体的には，第3.1節の失敗事例の原因の場合，マルウェアは悪意のあるソフトウェアへ，業務委託先のルール違反はセキュリティ意識の欠如へ，業務委託先の管理不徹底は不適切な要員管理へ，それぞれ対応付けを行った．

その結果を表 4に示す．原因が1つも対応付けされず，明らかに情報セキュリティとは無関係な小分類の項目は表記していない．しかし，今後，失敗事例を増加によって対応付けが予想される項目は，番号を付与せずに，そのまま記載した．その結果，下線を引いた 2 個の追加項目以外は，表 3の類型化へマッピングが可能であった．そして，55 個の原因は，小分類の 12 個の項目に分類が可能であった．

表 4 情報セキュリティ失敗事例の原因の類型化

大分類	中分類	小分類
1.技術的な要因で，しかもシステム/ソフトウェアに関わるエンジニアが少なくとも最初に考えるべき情報セキュリティ的な設計要因	1.バグ・セキュリティホール	1.ソフトウェアの故障(6件)，2.NW構成要素の技術的障害(1件)
	2.内部関係者を利用しない攻撃	3.トラフィックの過負荷(4件)，4.トラフィック/設定分析(4件)，メッセージ経路変更
	3.内部関係者を利用した攻撃	5.悪意のあるソフトウェア(17件)
2.技術的な要因だが，普通は副次的に考えている使用時の設計要因	4.想定外の制約	特殊使用(ユーザのエラーなど)，システム環境故障(停電，ハードウェアの故障など)
	6.火災・天災の影響	災害(火災，地震など)
	7.連鎖反応で拡大	6. ウィルス感染の拡大(3件)
	8.冗長系の非動作	フェイルセーフ不良，待機系不良
3.技術的な要因だが，人間や組織との関係が強い設計要因	9.作業で気を抜く	入力ミス(操作員のエラー)，保守作業ミス(保守のエラーなど)
	10.設計で気を抜く	流用設計，暗号や認証の欠如(保護されていない通信回線など)，物理的な保護の欠如(建物，ドアおよび窓の物理的保護の欠如)，記録の欠如(監査証跡の欠如など)，7.ルールが不十分(2件)
4.技術ではどうしようもない組織的な要因	11.個人や組織の怠慢	コミュニケーション不足，安全装置解除(離席時にログアウトしないなど)，8.不適切な情報管理(紛失，不十分なパスワード管理など)(7件)，9.不適切な要員管理(要員の不在など)(4件)，10.ルールの未整備(1件)
	12.悪意の産物	11.違法行為(盗難など)(1件)，12.倫理問題(不正なユーザによるNWへのアクセスなど)(5件)，テロ(破壊行動など)

5 考察と今後の課題

機械工学の分野における類型化である表 1 に基づき，情報セキュリティの脅威や脆弱性の例 68 個から表 3を作成し，そこへ収集した失敗事例の原因 55 個を対応付け，表 4を作成した．この原因のうち 94.5%が表 3の小分類の項目で対応付け可能であり，既存の類型化を利用したこれら項目の抽象度はある程度大きいといえる．ただし，この類型化の各項目の抽象度は小さ過ぎれば組織固有の項目となる可能性があり，大き過ぎれば単なる分類となる．この項目から，過去の失敗事例やそれらへの対応や対策などが引き出せる程度の抽象度が適切であり，この検証は今後の課題である．

また，今回の 55 個の原因では該当しなかった小分類の項目が存在した．そのため，今後も継続的に失敗事例を収集し，その原因を対応付けことによって，類型化の精度を向上させる必要がある．

本稿では，収集した情報セキュリティの失敗事例を他組織と共有可能とするために，原因の類型化という手段をとって知識化を試みた．今後は，この失敗事例の知識化の試みと，既存の失敗マネジメントシステムの考え方との関連性をさらに検討する必要がある．その上で，新しい失敗を予測する訓練や失敗が発生した際の，素早く，適切な対応の実施などへ，この失敗知識を活かす仕組みについて検討を進める．

参考文献

[1] JIPDEC: 情報セキュリティマネジメントシステム(ISMS)とは，(2006) http://www.isms.jipdec.or.jp/isms/index.html

[2] 経済産業省: 事業継続計画策定ガイドライン，(2005) http://www.meti.go.jp/policy/netsecurity/downloadfiles/6_bcpguide.pdf

[3] 畑村洋太郎: 失敗学のすすめ，講談社(2000)．

[4] 中尾政之: 失敗学 似たような失敗が思い出せるか，一橋ビジネスレビュー，Vol.54, No.3, pp.26-38 (2006)．

[5] 中尾政之: 失敗百選 41 の原因から未来の失敗を予測する，森北出版(2005)．

[6] 知見邦彦，櫨山淳雄，宮寺庸造: 失敗知識を利用したプログラミング学習環境の構築，電子情報通信学会論文誌，Vol.J88-D-I, No.1, pp.66-75 (2005)．

[7] JNSA: 2010 年 情報セキュリティインシデントに関する調査報告書 ー個人情報漏えい編ー，(2010) http://www.jnsa.org/result/incident/data/2010incident_survey_PIL_v1.3.pdf

[8] IPA: 情報セキュリティ教本，実教出版，(2010)，pp.103-104