情報処理学会論文誌 Vol.54 No.9 2208–2219 (Sep. 2013)

情報セキュリティの失敗事例における原因の類型化とその対策に関する考察

佐藤 亮太[1,†1,a)] 間形 文彦[1] 高橋 克巳[1] 桑名 栄二[1,†2]

受付日 2012年11月30日, 採録日 2013年6月14日

概要：企業や大学などの組織における情報セキュリティに関する事故や事故にまでは至らないヒヤリハットの事例が多発している．そのため，事故やヒヤリハットなど情報セキュリティの失敗に対する適切な対応が，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，次の新たな設計への出発点とする研究が存在する．本稿では，一般的には公表されにくい，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，その原因を，機械工学と情報セキュリティにおける原因の考え方の差分を明らかにしながら，機械工学における類型化の方針に沿って分析する．さらに，その分析結果として得られた類型化が，失敗学の思想を反映して，情報システムの運用者を対象とした既存の ISMS とは異なった，情報システムの設計者を対象とした情報セキュリティ対策を実現する手段となることを述べる．そして，失敗事例のうち，同じ類型化をされた事例における対策を相互参照することで，1 つの失敗事例では実施されなかった新たな対策案が提示可能となることを示す．さらに，失敗事例の分析において，リスク表現におけるリスク源，事象，結果の関係性に対するリスク対応の考え方を導入することで，情報システムの設計者の立場からの新たな技術的対策の観点を導出し，本稿による事例ベースの原因分析とその対策関連の導出による新たな失敗マネジメントの有効性を示す．

キーワード：情報セキュリティ，失敗学，インシデント

A Study of a Classification for Causes of Information Security Incidents and Countermeasures for their Causes

Ryota Sato[1,†1,a)] Fumihiko Magata[1] Katsumi Takahashi[1] Eiji Kuwana[1,†2]

Received: November 30, 2012, Accepted: June 14, 2013

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. In the study of failures, there is an approach which classifies the failures based on their causes to derive the knowledge. In this paper, we collect the cases of the failures in information security and classify their causes based on the way of the study of failures in clarifying the differences of causes between engineering and information security. As a result, we discuss that the classification is the way for the designer of information security system to control for causes, and is different from ISMS, which is the way for the operator of the system. We demonstrate the classification's effectiveness by showing new controls derived from other cases which are classified with same category. In addition, we introduce the way of risk management for the relationship among risk sources and their event and its consequence to derive the controls for the designer of information security.

Keywords: information security, the study of failure, incident

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 Web ページの改ざんや従業員などによる電子機器の紛失にともなう機密情報の漏えい，オペレータの誤操作によるデータの消失など，情報セキュリティにまつわる事故や事故にまでは至らないヒヤリハットの事例が後を絶たない．このような事故やヒヤリハットなど情報セキュリティの失敗（詳細な定義は 3.2 節を参照）に対する適切な対応が，各組織の事業継続にとって重要な課題となっている．

そこで，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に，ISMS（Information Security Management System）の構築などの対応がとられている [1]．ISMS は，国際規格である ISO/IEC 27001:2005 として規定されており [2]，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，情報システムを運用するための仕組みである．

ISMS による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と考えられる．しかし，一般的には，組織内で発生した情報セキュリティの失敗事例や教訓を組織外へと積極的に情報公開されることが少ない．たとえば，内部不正行為による情報セキュリティの失敗事例については，それらの失敗事例を公的・中立的機関へ情報提供するかという問いに対し，公開するが 9%であり，公開しないが 32%という結果がある [3], [4]．つまり，失敗事例や教訓を，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．

一方，「失敗事例から新たな教訓を学び，次へ活かす」という思想を持つ失敗学が注目されている [5]．そこでは，様々な失敗事例の原因分析から，共通した原因を抽出することで抽象化し，失敗事例からのいわゆる教訓としている．そして，その教訓は，**図 1** に示すように，他組織も含んだ次の組織活動へ展開されることにより，新たな失敗の再発防止が可能とされている [6]．

また，ISMS は，対象となる情報システムの運用を適切に実施するための仕組みであるため，情報システムの運用者を主な利用対象としている．ISO/IEC 27002:2005 においては [7]，ISMS 実践のための規範として，情報セキュリティの失敗を発生させないための，運用者に向けた管理策がまとめられている．ただし，情報システムの設計者に向けられた管理策ではないため，情報セキュリティの失敗が生じた際に，それに対して設計者が対策を考案するための直接的な指針にはなっていない．

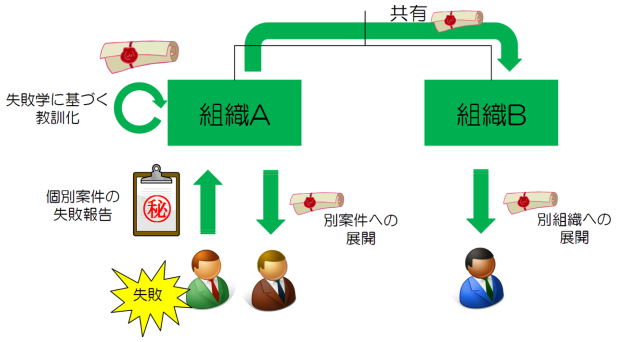

図 1 失敗学における教訓の展開
Fig. 1 Usage of a lesson on the study of failure.

表 1 失敗学と ISMS との比較
Table 1 Comparison of the study of failure with ISMS.

	失敗学	ISMS
対象者	製品/情報システムの設計者	製品/情報システムの運用者 製品/情報システムの利用者
対策	設計対策	運用対策
適用範囲	失敗の発生した組織 失敗の発生していない他の組織	失敗の発生した組織

一方，上述した失敗学は機械工学の分野を起源として発展しており，特に，機械工学における失敗事例を約 200 件収集，詳細に事例発生の経過を分析した結果，それらを 41 の失敗原因で類型化している [8], [9]．さらに，その失敗原因は，主に設計者の観点から類型化がされており，その類型化に基づいた設計段階における対策が検討されている．

表 1 にまとめたとおり，失敗学に基づく失敗に対するマネジメントは，その主な対象者や対策段階，適用範囲において ISMS とは異なっている．そのため，失敗学の考え方を情報セキュリティの分野へ援用することによって，既存の情報セキュリティにおける失敗マネジメントとは異なる視点を持つ，新たな失敗マネジメントが導出されると期待できる．しかしながら，情報セキュリティにおいて，詳細分析が可能な失敗事例を多く収集することは，前述のとおり，一般的には困難と考えられ，同様な類型化の方針に基づいて情報セキュリティの失敗事例の原因を類型化する試みはこれまでされていない．

本稿では，一般的には公表されにくい情報セキュリティの失敗事例を収集し，その原因を，機械工学と情報セキュリティにおける原因の考え方の差分を明らかにしながら，機械工学における類型化の方針に沿って分析する．さらに，その分析結果として得られた類型化が，失敗学の思想を反映し，情報システムの運用者を対象とした既存の ISMS とは異なり，情報システムの設計者を対象とした実例ベース

[1] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, NTT Corporation, Musashino, Tokyo 180–8585, Japan
[†1] 現在，日本電信電話株式会社技術企画部門
Presently with Technology Planning Department, NTT Corporation
[†2] 現在，NTT Innovation Institute Inc.
Presently with NTT Innovation Institute Inc.
[a)] ryota.sato@hco.ntt.co.jp

の情報セキュリティ対策を実現する手段となりうることを示す．続いて，失敗事例のうち，同じ類型化をされた事例における対策を相互参照することで，1つの失敗事例では実施されなかった新たな対策案が提示可能となることを示す．さらに，失敗事例の分析において，リスク表現におけるリスク源，事象，結果の関係性に対するリスク対応の考え方を導入することで，情報システムの設計者の立場からの新たな技術的対策の観点を導出し，本稿による事例ベースの原因分析とその対策関連の導出による新たな失敗マネジメントの有用性を示す．

2. 関連研究

前述のとおり，失敗学は，主に機械工学の分野で発達している [5]．失敗学においては，たとえば，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1つの行為が，はじめに定めた目的を達成できないこと」と定義したうえで，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．具体的には，様々な失敗事例の原因分析から，共通した原因を抽出することで抽象化し，失敗事例からのいわゆる教訓としている．その教訓の具体例として，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 [8], [9]．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主に設計者の立場から抽出している．その結果，**表 2** に示す，41分類に類型化できるとしている．この類型化で注目すべきは，失敗原因の大分類が，「設計要因」を中心に分けられている点である．失敗を次の「設計」に活かすという失敗学の思想が原因の分類にも表れている．

さらに，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 [10]．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事例の持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．

また，情報セキュリティの失敗事例の原因に対する類型化に関しては，特に内部不正に起因する事例において研究が進んでいる．米国においては，CERT/CC（Computer Emergency Response Team Coordination Center）の Insider Threat Center [11] によって，内部不正に関わる事例に関する詳細な研究がされており，内部不正の事例を「Employee Fraud」，「Theft of Information」，「IT Sabotage」の3分類でまとめている [3], [12], [13]．また，国内においては，日本の警察機関の有する事件資料から内部不正に関わる30件の事例調査を行い，類型化などにより事案発生過程およびその原因を把握し，対策を検討がされている [14]．参考文献 [14] の類型化では，内部犯行者による事例を Insider Threat Center による研究と同様に「システム破壊」，「システム悪用」，「情報流出」の3つの様態に分類し，さらに「道具的な犯行」，「表出的な犯行」の2つの犯行タイプの観点を考慮して，情報流出を「情報流出 I（道具的な犯行）」と「情報流出 II（表出的な犯行）」と類型化している．

表 2 失敗学における失敗原因の類型化
Table 2 Classification of causes on the study of failures.

大項目	中項目	小項目
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.火災避難，22.天災避難，
	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

一方で，失敗学が取り扱う失敗をリスクととらえると，リスクを扱う関連学問としてリスク学が存在する [15]．リスク学においては，経済や法律，環境などの様々な分野を対象に研究が進められており [16], [17], [18]，個々の分野でリスクの定義などは異なるものの，リスク指標やリスク評価，リスクマネジメントなどリスクを扱うための方式や技術が議論されている．特に，安全の分野では，広く人工物またはその影響によってもたらされ，自然現象，組織活動の欠陥，ヒューマンエラーなどにより発生するリスクを対象に，「安全—危険」，「安心—不安」，「満足—不足」という軸から問題解決を図ろうとする安全学がある [19]．また，IT 分野では，情報セキュリティに加えプライバシや IT システムの信頼性・安全性を対象として，それらに関わる IT システムの安全が損なわれる可能性を「IT リスク」と定義し，その IT リスクを低減させるための方式や技術を体系化した IT リスク学がある [20]．

これらリスク学，安全学，IT リスク学は，事故や被害や損失が生じるリスクを，「想定される影響の規模」と「その影響が生じる確率」として評価し，評価したリスクを受容可能な水準までコントロールする学問である．一方，失敗学は，広くものづくりにおいて発生した失敗事例における原因を分析・究明し，個々の原因や事例を抽象化された知識に昇華することで教訓とし，ここで得られた教訓を別の具体的事例に応用することを通して，同じ失敗を繰り返さ

ないための学問である．

前者と後者では，対象とするリスクの範囲，アプローチ方法やとらえ方，学としての体系化の方法などが大きく異なっている．

3. 情報セキュリティにおける失敗とその事例

3.1 失敗学における失敗事例とその類型化の具体例

失敗学の考え方を援用して，情報セキュリティの失敗事例の原因を類型化する前に，失敗学が主に対象としていた機械工学の分野における失敗事例とその分析の例について述べる．参考文献 [6] にも記載されている「三井三池炭鉱の炭塵爆発」は，1963 年，炭鉱において石炭の粉が空気中に浮遊しており，それが何らかの理由で着火，爆発し，死者 458 名，重軽傷者 555 名を出した事例である．こうした失敗事例に対し，表 2 の類型化を実施した参考文献 [8] においては，いわゆる報告書のように長い文書で内容を表現するのではなく，シナリオのように短い文書で時系列に内容を記載している．こうした記載方法により，失敗事例における原因，結果，対策などの分析がしやすくなるとしている．そして，上記事例のシナリオの分析から，結果として「爆発によって死傷者がでた」を，対策として「常に清掃し，水を撒いて湿らせておく」を抽出している．また，原因を抽出する際には，たとえば「炭塵が静電気など何らかの理由で着火」と事例固有の表現ではなく，「(炭塵を始めとする) 紛体は表面積が多いので爆発的に酸素と結びつき爆発」などと原因を抽象化する．その抽象化された原因が，表 2 に記載されている「18. 塵埃」として類型化されている．

つまり，たとえば個別事例である炭塵爆発の事例と原因のみが記載された失敗の報告書のみでは，その事例で実施された対策などを参照し，次の失敗の防止に活かせる者は炭鉱など炭塵を扱う者のみに限定される．一方で，塵埃と類型化された失敗は，たとえば工場の排気ダクトの設計者が，油分を含んだ埃を扱う排気ダクトの設計において，炭塵爆発の事例とその対策を参照し，次の失敗の防止に活かすことができるようになる [6]．

3.2 情報セキュリティにおける失敗の定義

失敗学の考え方を援用して，情報セキュリティの失敗事例の原因を類型化するために，情報セキュリティの失敗について定義をする．そのために，リスクマネジメントに関する国際標準 ISO/IEC 31000:2009 に着目する [21]．ISO/IEC 31000:2009 は，情報セキュリティだけではなく，機械や環境，医療など特定の分野に限らないリスク一般を対象としたリスクマネジメントの規格である．

ISO/IEC 31000:2009 において事象は，「ある一連の周辺状況の出現又は変化」，結果は，「ある目的に影響を与える事象の結末」，と定義されている．つまり，**図 2** に示すように，事象と結果は因果の関係で結ばれている．本稿においては，事象と結果の因果関係を情報セキュリティに適用し，情報セキュリティにおける失敗を定義する．情報セキュリティの C.I.A，すなわち，ある組織の持つ情報資産に対する機密性 (Confidentiality)，完全性 (Integrity)，可用性 (Availability) を脅かす事象によって引き起こされる C.I.A を損なう結果の発生を「情報セキュリティにおける事故」と定義し，結果にまでは至らない事象の発生を「情報セキュリティにおけるヒヤリハット」と定義する．そして，事故とヒヤリハットを含むものを情報セキュリティにおける失敗と定義する．

図 2 リスク表現におけるリスク源と事象と結果の関係

Fig. 2 Relationship among risk sources and their event and its consequence.

また，その事象を引き起こす要素としてリスク源が存在する．リスク源は「それ自体又はほかとの組み合わせによって，リスクを生じさせる力を本来潜在的に持っている要素」と定義される．本稿では，このリスクの因果関係で示されるリスク源を具体的な情報セキュリティの失敗事例から抽出し，そのリスク源に対する類型化を実施する．

3.3 情報セキュリティにおけるリスク源

情報セキュリティにおける失敗の原因であるリスク源には，**表 3** に例示する，脅威と脆弱性の考え方がある [22]．脅威は「システムまた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 [23]．そして，情報セキュリティの事象は，脅威と脆弱性が組み合わさって発現すると考えられている．

一方で，機械工学の分野におけるリスク源の類型化である表 2 においては，その小分類にリスク源が記載されているものの，リスク源を脅威と脆弱性に分ける観点に基づいた分類とはなっていない．しかし，脅威と脆弱性の観点から表 2 を改めて分析すると，小分類の各項目は脅威，脆弱性，または脅威と脆弱性の組合せのいずれかであることが分かる．たとえば，「13. 強風」は橋への振動を引き起こす自然現象であり，崩落事故をもたらす脅威である．「29. 待

表 3 脅威と脆弱性の例
Table 3 Examples of threats and vulnerabilities.

人為的脅威の例		環境的脅威の例
意図的脅威	偶発的脅威	
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	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	地震，台風，落雷，ほこり，静電荷，記憶媒体の劣化
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，トラフィックの過負荷，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		
	電力の不安定	
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		

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，送信元および受信者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

機系不良」は，冗長化された装置が待機系に切り替わらない欠陥を指し，装置の信頼性を損なう脆弱性である．「1. 脆性破壊」は材料自体の脆さという脆弱性に，引張り応力の存在などの脅威が組み合わされて生じる破壊現象である．このように，脅威と脆弱性の観点からリスク源を分類する考え方は，機械工学の分野においても有効である．

したがって，表 2 を参考としながら情報セキュリティの失敗事例のリスク源を類型化する際は，情報セキュリティのリスク源に対する基本的な考え方である脅威と脆弱性の観点を導入する．たとえば，意図的な人的脅威として，組織外の脅威源の場合は DDoS 攻撃，組織内の脅威源の場合は内部不正などが存在することを考慮して類型化を進めることとなる．

3.4 情報セキュリティの失敗事例

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独自に収集し [24]，さらに，Web や雑誌などで掲載された失敗事例を合わせて 50 件収集した．本節では，事故事例のうち最も多かった悪意あるソフトウェアに関する事例を機密性，可用性の観点から 2 件とヒヤリハットの事例を 1 件の計 3 件を例示する．例示にあたっては，3.1 節で述べた失敗学における失敗事例の記載方法を採用し，各失敗事例の内容を時系列に短い文書で記載する．

(1) 顧客端末へのウィルス感染拡大

［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 カ月］感染経路などの調査に 1 カ月を要した．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］

(2) Winny 経由で機密情報漏えい

［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 社において，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，経営者会議において，モニタリング継続との対応を決定．

［n 日 + 1 カ月］某掲示板サイトにおいて，A 社機密情報の投稿を予告する書き込みが発生．

［n 日 + 5 カ月］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］

(3) Web サイトのコーディングミス

［n 日］A 社の社外向け Web サイトの画像認証（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］

4. 情報セキュリティの失敗原因の類型化

前章では，我々が収集した 50 件の情報セキュリティにおける失敗事例のうち 3 件を例示した．本章では，失敗学における類型化の方針にならって，50 件の失敗事例における原因の類型化を試みる．

4.1 類型化の目的

前述のとおり，情報セキュリティの失敗事例は，組織の外へ公開されることが少なく，たとえば，組織内において

表 4 脅威と脆弱性の失敗学の類型化への対応付け
Table 4 Corresponding to causes on the study of failures and examples of threats and vulnerabilities.

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	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，通信への侵入，保護されていない通信回路，送信元および送信者の識別と認証の欠如
	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，18.塵埃・動物，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	21.火災(火事)，22.天災(地震など)
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)
	10.設計で気を抜く	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)
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	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(文書化の欠如など)，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)，40.倫理問題(不適切な採用手続き)，41.テロ(破壊行動など)

はある種の機密情報として管理される場合もあり，他組織へ展開されにくい．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ない場合があり，有用な情報として活用されない可能性がある [6]．そこで，複数の失敗事例に含まれる共通の原因を，他組織の事例へも演繹可能な類似点として抽出する類型化が有効となる．さらに，表 2 のような，原因に基づく類型化の各項目に対し，具体的な対策とまではいかないまでも，対策の方針が対応付けられれば，図 1 にも示したとおり，他組織においても普遍的な教訓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 2 に示す，失敗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．その際，3.3 節で述べたとおり，失敗学と情報セキュリティにおけるリスク源に対する考え方の違い反映させる．具体的には，情報セキュリティにおけるリスク源に対する基本的な考え方である脅威と脆弱性の観点を，表 2 へ反映させる．

そこで，表 3 に示す 68 個の脅威と脆弱性の例について，機械工学におけるリスク源が記載された表 2 の小分類の各項目へ対応付けを行った．表 3 の例は，ISO/IEC TR 13335:1997 が示した脅威と脆弱性の例として [25]，参考文献 [22] に記載されているものである．なお，3.1 節で述べたとおり，失敗学においてはリスク源を抽象化した表現で記載することで，個別事例から他の事例へ対策などの演繹が可能となる．ISO/IEC TR 13335:1997 が示す脅威と脆弱性の例は，個別事例のリスク源として表現されているのではなく，抽象化されたリスク源として表現されており，情報セキュリティ失敗事例の原因の類型化の項目として適切と考えられる．

表 3 に示す 68 個の脅威と脆弱性の例について，表 2 の小分類の各項目へ対応付けにあたっての方針は下記のとおりである．

- 大分類 1，2 には，脅威の主体が組織外となる意図的な人為的脅威の例を含める．
- 既存の大，中，小項目については，可能な限りそのままの項目として例の対応付けを行う．対応付けが可能であった例は，その小項目へ括弧付けで記載する．
- 既存の大，中，小項目において，表現に変更が必要な項目や項目そのもの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．

対応付けの結果を**表 4** に示す．下線部は表 2 から新たに修正，追加された項目であり，複数の脅威や脆弱性の例が同一の既存小項目へ対応付けられる場合，代表的な例を括弧内に記載している．詳細な対応付けの結果については付録 A.1 に記載している．また，付録 A.1 において情報セキュリティの脅威や脆弱性と対応付けがされなかった中分類，小分類の項目（N/A と記載）に関しては削除している．

表 4 の結果から，表 2 において，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は情報システムの利用者/運用者が注意すべき項目が多いことが分かる．一方，技術的な要因が関係する項目，つまり，大分類 1，2 は，設計者が注意すべき項目が多い．そのため，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，すべ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．

4.3 情報セキュリティ失敗事例のリスク源の導出

表 4 に基づいて，3.4 節において述べた失敗事例を含む 50 件の失敗事例のリスク源の類型化を行う．各失敗事例におけるリスク源の分析においては，3 章で述べたリスクの考え方に基づいてリスク源を導出した．このとき，1 つの失敗事例に対して，そのリスク源は複数存在する場合もあるが，直接的に事象を発生させたと考えられるリスク源 1 つに絞っている．また，リスク源のうち，脅威と脆弱性が必ずしもともに判明していない事例も含まれている．具体的なリスク源の分析結果として，3.4 節で示した 3 つの失敗事例について例示する．

失敗事例 (1) は，「業務の停止/遅延」という可用性を損な

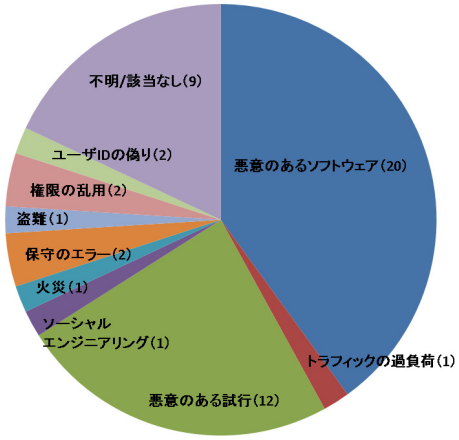

図 3 失敗事例における失敗原因（脅威）の割合
Fig. 3 Proportion of threats in information security failures.

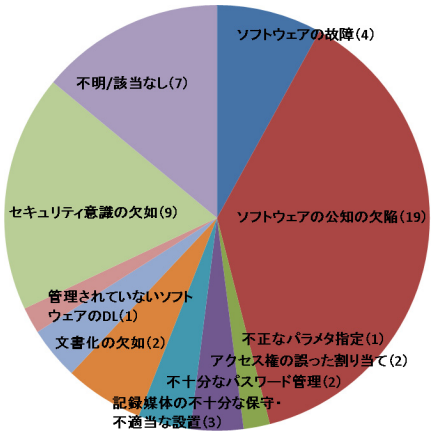

図 4 失敗事例における失敗原因（脆弱性）の割合
Fig. 4 Proportion of vulnerabilities in information security failures.

う結果である．また，この結果をもたらした事象は「ウィルスの感染」である．そして，リスク源は，脅威の観点からは「悪意のあるソフトウェア」であり，脆弱性の観点からは，作業における個人所有の USB 媒体利用に関する文書化がされていなかったとして「文書化の欠如」である．

失敗事例 (2) は，「情報漏えい」という機密性を損なう結果である．また，この結果をもたらした事象は「ウィルスの感染」である．そして，リスク源は，脅威の観点からは「悪意あるソフトウェア」であり，脆弱性の観点からは，Winny の利用禁止はルールとして文書化もされていたため従業員の「セキュリティ意識の欠如」である．

失敗事例 (3) において，結果は「なし」である．つまり，失敗事例 (3) はヒヤリハットの事例であり，組織の情報セキュリティを損なう結果は発生していない．ただし，情報セキュリティを脅かす事象として「不正な認証によるアクセスが可能な状態」が発生している．そして，リスク源は，脅威の観点からは，結果が発生していないため脅威は「なし」であり，脆弱性の観点からは，ソフトウェアとしての潜在バクとして「ソフトウェアの故障」である．

上述した 3 つのリスク源の導出と同様の分析を，失敗事例 50 件に対して実施し，その結果として脅威 41 個と脆弱性 43 個を合わせて 84 個（不明/該当なしを除く）のリスク源を抽出した．その結果を**図 3**，**図 4** に示す．

ここで，表 4 の項目には該当しない脅威が存在したため，ISO/IEC 27005:2011 の Annex C に記載の例から「権限の乱用」を追加し [26]，さらに，ISO/IEC 27005:2011 の Annex C においても適切な例がない脅威について，「悪意ある試行」，「ソーシャルエンジニアリング」を新たに追加した．また，脆弱性についても同様に「ソフトウェアの公知の欠陥」と「不正確なパラメータ指定」を新たに追加している．

脅威においては，いわゆるウィルスによる脅威が 20 個と最も多く，SQL インジェクションなどの脆弱性を狙った悪意ある試行が 12 個と続く結果となった．つまり，脅威においては上位 2 つのリスク源が全体の約 78%を占めており，多くの失敗事例において類似のリスク源であったといえる．一方，脆弱性においては，サーバソフトウェアなどの既知の脆弱性の放置などのソフトウェアの公知の欠陥が 19 個と多く，続いては，委託先を含む従業員のセキュリティ意識の欠如が 9 個となった．つまり，脆弱性においては上位 2 つのリスク源が全体の約 65%を占めており，図 3 に記載の脅威の結果を比較すると，失敗事例ごとにある程度異なるリスク源であったといえる．

上記 84 個のリスク源を，表 4 へ対応付けた結果を**表 5** に示す．ここで，括弧内には対応付けられたリスク源の個数が記されている．表 5 の結果から，実例として発生している情報セキュリティの失敗事例におけるリスク源の多くが，大分類 1，2 に分類されていることが分かる．失敗学においては，その教訓を反映すべき対象として機械の設計者を想定しており，その設計者がより意識すべき設計要因が分類 1，2 である．つまり，情報セキュリティにおいても，情報システムの設計者が，情報システムの設計段階から，過去の教訓から学んだ脅威や脆弱性に対する対策を組み込むことが重要となることを示している．

特に，図 3，図 4 において，上位のリスク源が失敗学の大分類 1，2 に対応付けられている．これは，情報セキュリティにおいて設計者が，設計段階から情報セキュリティ対策をすることの重要性をより強く示した結果といえる．

また，この結果は，表 1 においても示したように，既存の ISMS が情報システムにおける利用者/運用者に対するセキュリティマネジメントであることに対し，失敗学を取り込んだ本研究は，情報システムにおける設計者に向けたセキュリティマネジメントとなることを示している．つまり，ISMS と本研究は相補的な関係となることが分かる．

5. 情報セキュリティ失敗事例の類型化の評価

前章では，我々が収集した情報セキュリティにおける失

表 5 情報セキュリティ失敗事例の原因の類型化
Table 5 Classification of causes in information security failures.

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	バグ・セキュリティホール	ソフトウェアの故障(4件)，NW構成要素の技術的障害，ソフトウェアの公知の欠陥(19件)
	内部関係者を利用しない攻撃	トラフィックの過負荷(1件)，トラフィック分析，メッセージ経路変更，通信への侵入，保護されていない通信回路，送信元および送信者の識別と認証の欠如，悪意ある試行(12件)
	内部関係者を利用した攻撃	悪意のあるソフトウェア(20件)，ソーシャルエンジニアリング(1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	想定外の制約	特殊使用(ユーザのエラーなど)，.落下物・付着物，塵埃・動物，システム環境故障(停電，ハードウェアの故障など)
	火災・天災の影響	火災(火事)(1件)，.天災(地震など)
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	作業で手を抜く	入力ミス(操作員のエラー)，保守作業ミス(保守のエラー，不正確なパラメタ指定など))(10件)
	設計で気を抜く	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)
4.技術ではどうしようもない組織的な要因	個人や組織の怠慢	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(文書化の欠如など)(3件)，不適切な要員管理(セキュリティ意識の欠如など)(9件)，ルールの未整備
	悪意の産物	違法行為(盗難，権限の乱用など)(4件)，倫理問題(不適切な採用手続き)，テロ(破壊行動など)

敗事例に対し，失敗学における類型化を出発点として，それら失敗事例のリスク源を分類した．その結果より，多くのリスク源が設計者の観点から考慮すべき設計要因であることを示した．

本章では，類型化された各リスク源に対応する情報セキュリティの失敗事例において実施された複数の技術的な対策を示し，それら対策が別の事例において参照されることの有用性について述べる．さらに，失敗学に基づく類型化からの重要な示唆である設計者の観点からの設計対策を検討するために，3 章において紹介したリスク分析の枠組みを導入し，既存の運用者向けの対策とは異なる設計者向けの対策案が導出できることを示すことで，本研究の有用性について述べる．

5.1 悪意あるソフトウェアに関わる事例における対策

情報セキュリティの失敗事例の脅威に関するリスク源として最も多かった悪意あるソフトウェアに着目する．実際の失敗事例において実施された具体的な技術的対策は，下記 3 点に大別できる．

- 導入済みのパターンファイル型のウィルス対策ソフトのパターンファイルを最新化する．
- 検知の精度を高める目的で，複数のパターンファイル型ウィルス対策ソフトを導入する．
- 最新のパターンファイルでも検知できない場合に備え，振舞い検知型のウィルス対策も導入する．

どの事例においても，上記 3 つの対策すべてが実施されたものはなく，それぞれの事例の特徴に合わせた対策が実施されている．ただし，ある 1 つの事例においては，導入済みウィルス対策ソフトが，最新パターンファイルを適用済みであったにもかかわらず，ウィルスの検知ができなかったため，複数ウィルス対策ソフトの導入を行っている．この事例においては，上記 3 番目の振舞い検知型ウィルス対策ソフトの導入検討が行われたかどうかは記録が残っていないため不明であるが，もし検討されていない場合は，費用対効果も勘案し，導入検討されることが望ましい．上述のとおり，過去の事例で実施された対策を教訓として参照できることは，たとえば他の組織において発生した同様の失敗に対して適切な対策を実施するうえで有用といえる．

ただし，上記 3 つの対策に関しては ISO/IEC 27002:2005 [7] における管理策 10.4.1 悪意のあるコードに対する管理策に同様の記載が存在している．たとえば，当該管理策 10.4.1 の「関連情報」において，「保護内容が最新のものであることを確実にするために，定義ファイル及びスキャンエンジンの自動更新を可能とする」や「異なるベンダから供給される二つ以上の，悪意のあるコードからの対策ソフトウェア製品の利用」などの記載がある．これらは情報システムの運用者における対策案である．実際の失敗事例においても，ISO/IEC 27002:2005 の管理策を参考とし，運用者向けの対策を実施したと考えることもできる．

5.2 リスク対応の観点による分析

前節においては，リスク源として悪意あるソフトウェアに着目し，同じリスク源を持つ他の情報セキュリティの失敗事例において実施された対策が，別の事例において参照されることの有用性について述べた．しかし，上述した 3 つの対策は ISO/IEC 27002:2005 にも記載された運用者向けの対策であり，4.3 節の結果から示された失敗学からの重要な示唆である設計者向けの設計対策とはなっていない．

失敗事例に基づいて，設計対策を抽出するためには，失敗事例におけるリスク源（設計要因）に対する設計対策の観点を示し，その観点からの具体的な設計対策案を検討する必要がある．そこで，3 章において述べたリスクマネジメントにおけるリスク対策の考え方を導入し，リスク源に対する対策の観点を示す．ISO/IEC 31000:2009 [21] においては，下記 7 項目をリスク対策の観点として整理している．

- リスクを生じさせる活動を，開始または継続しないと

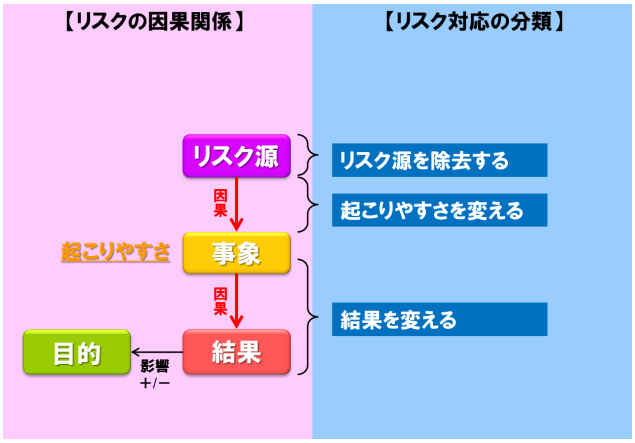

図 5 リスクの因果関係とリスク対策の観点の分類
Fig. 5 Classification of controls for risk sources.

決定することによって，リスクを回避する．
- ある機会を追及するために，リスクをとるまたは増加させる（＋の影響の場合）．
- リスク源を除去する．
- 起こりやすさを変える．
- 結果を変える．
- 1 つ以上の他者とリスクを共有する（契約およびリスクファイナンシングを含む）．
- 情報に基づいた意思決定によって，リスクを保有する．

上記のうち，設計者の観点において考慮すべき項目は，リスク源を除去する，起こりやすさ変える，結果を変える，の 3 点である．これら 3 つのリスク対策の観点と図 2 に記したリスクの因果関係との関連を図 5 に示す．

上記 3 つの観点から悪意あるソフトウェアという脅威に対する設計対策を検討する．

「リスク源を除去する」の観点からは，ウィルスなど悪意あるソフトウェアそのものの存在を消す方法が考えられる．ただし，ウィルスなど悪意あるソフトウェアそのものの存在を消すような技術的な対策は現状のところ存在しておらず，刑罰を科するなどのリスク源を生み出す者に対する抑止策が存在するのみである．

「起こりやすさを変える」の観点については，まさにウィルス対策ソフトが技術的対策である．つまり，ウィルス感染という事象を起こりにくくする観点から，ウィルス対策ソフトを開発する場合は設計者による設計対策，開発済みのウィルス対策ソフトを導入し，「保護内容が最新のものであることを確実にするために，定義ファイルおよびスキャンエンジンの自動更新を可能とする」や「異なるベンダから供給される 2 つ以上の，悪意のあるコードからの対策ソフトウェア製品の利用」をする場合は運用者による対策である．

「結果を変える」の観点からは，ウィルス感染という事象が発生した後でも，情報漏えいやシステム停止などの結果を出さない対策が考えられる．失敗学では，故障という事象が発生しても安全な状態を維持して最悪の結果に至らないフェールセーフや要求機能の遂行を維持するフォールトトレランスといった設計手法が常識である．こうした手法を適用すれば，ウィルス感染の発生後，外部への情報送信が行われる前に送信パケットを自動的に遮断し機密性を維持するソフトウェアや，ウィルス感染後にシステムが停止しても冗長系に切り替わり，可用性を維持する冗長システムなどの設計案が導出できる．パケット送信の自動遮断やシステムの冗長化は，いずれも運用者向けの ISO/IEC 27002:2005 [7] には見られない設計対策案である．

「結果を変える」とは，結果を出さないだけでなく，結果を小さくすることも含まれる．システムが停止しても，速やかに修復して復旧すれば，可用性が大きく損なわれるのを抑えることができる．失敗学では，故障が発生した後の修復のしやすさにも留意した保全性設計を設計者に求めている．設計段階で保全性に留意するならば，たとえば，悪意あるソフトウェアによってシステムが改ざんされることを想定して，改ざん検知ができる仕組みを用意し，バックアップデータを取得するだけでなく，さらにバックアップデータを丸ごと格納したディスクと容易に交換・換装できるようにハードウェアを設計するなどの修復の容易さと短時間での復旧を目指したバックアップシステムの設計案が導出される．

改ざん防止や媒体のバックアップならば，ISO/IEC 27002:2005 などでよく知られた対策例であるが，保全性設計に対する示唆は ISO/IEC 27002:2005 には見られない．

5.3 ソフトウェアの公知の欠陥に関わる事例における対策

5.1 節，5.2 節において，情報セキュリティの失敗事例の脅威に関するリスク源として最も多かった悪意あるソフトウェアという脅威に対する対策について述べた．本節においては，情報セキュリティの失敗事例の脆弱性に関するリスク源として最も多かったソフトウェアの公知の欠陥に着目し，その対策について考察する．ソフトウェアの公知の欠陥に関わる事例としては，SQL インジェクションに代表されるソフトウェアやそれを利用したサーバなどの脆弱性に起因する情報漏えい事例などがある．実際の失敗事例において実施された具体的な技術的対策は，下記 2 点に大別できる．
- OS やソフトウェアを，脆弱性を含まない最新のバージョンに更新する．
- IP フィルタリングなど，サーバなどへのアクセス可能端末を制限する．

実施された対策の詳細が不明な事例を除き，すべての事例において 1 番目の対策が実施されている．しかし，2 番目の対策がされていない事例もあり，もし，検討がなされていない場合は，各事例の特徴に合わせて 2 番目の観点からの対策検討されることが望ましい．5.1 節でも述べたと

おり，過去の事例で実施された対策を教訓として参照できることは，たとえば他の組織において発生した同様の失敗に対して適切な対策を実施するうえで有用といえる．

さらに，5.2 節で述べたリスク対応の観点から設計者向けの設計対策について分析すると，「リスク源を除去する」の観点からは，SQL インジェクションなどの脆弱性への対処が考えられる．たとえば，ウェブサーバの運用・管理者向けの SQL インジェクション対策としては，バインドメカニズムやエスケープ処理がよく知られており，ウェブアプリケーションのシステムに組み込む段階で行うこととされている．これは上述した 1 番目の対策に相当する．

一方，失敗学においては，人為的に不適切な行為や過失があっても信頼性を保持する設計手法であるフールプルーフの適用を考える．設計者の立場で設計段階からフールプルーフの設計方式を検討するならば，ウェブサーバの運用・管理者がバインドメカニズムやエスケープ処理を怠ったとしても脆弱性が生じないような製品の設計案が導出できる．たとえば，最初からバインドメカニズム，エスケープ処理，入力値のコントロールなどの仕組みを持ったウェブアプリケーションやアドオンプログラムの設計などが考えられる．

ISO/IEC 27002:2005 からは，不適切な行為や過失を減らすための組織的な対策のヒントは得られるが，失敗学が教える，不適切な行為や過失の発生を前提とした設計についての示唆は得られない．

上述のとおり，情報セキュリティにおける失敗事例において，リスクの因果関係とそのリスク対策の観点を導入することで，失敗事例に基づいた設計者の立場からの設計対策案の導出ができた．つまり，失敗学によりその重要性が示唆された設計段階からの対策は，リスクマネジメントの考え方に基づき検討可能であり，かつ検討された設計対策案は，前節で述べた具体的な失敗事例においては実施されなかった設計者向けの新たな対策案となることが示された．

なお，導出された設計対策案のうち，どれを優先的に採用すべきかについては失敗学の類型化を援用した本稿のアプローチでは示されない．設計対策案の採用にあたっては，対策案の設計への組み込み容易性や費用などの観点をもとに個別事例ごとに検討される．つまり，対策の導入容易性や費用といった観点に基づいた対策案の優先順位付けは，たとえば，採用する個別の組織における設計者の技術力や対策費用などに依存しており，類型化という個別事例からの抽象化などを行う本アプローチでは示されない．

6. まとめ

本稿では，組織における情報セキュリティの事故や事故にまでは至らないヒヤリハットといった情報セキュリティの失敗に対する適切な対策を実施するため，機械工学の分野において発展が見られる失敗学に着目し，失敗事例を原因に基づき類型化し，次の新たな設計への出発点とする考え方を情報セキュリティの分野に導入した．

一般的には公表されにくい，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 50 件収集し，その原因を，リスク表現におけるリスク源，事象，結果の関係性を導入し，分析した．その際に，機械工学と情報セキュリティにおける原因の考え方の差分として，脅威や脆弱性の概念を導入し，機械工学における類型化の方針に沿って分析した．

その結果として得られた情報セキュリティにおける失敗原因の類型化から，失敗事例における原因の上位が，設計者によって考慮されるべき原因（設計要因）であることが示され，設計段階からの情報セキュリティの対策の検討の重要性を示した．この結果から，失敗学の思想を反映した本稿の検討は，情報システムの運用者を対象とした既存の ISMS とは異なり，情報システムの設計者を対象とした実例ベースの情報セキュリティ対策を実現する手段であることも示した．

また，失敗事例の原因として悪意あるソフトウェアとソフトウェアの公知の欠陥に着目し，同じ原因を持つ失敗事例における対策が相互参照されることで，ある失敗事例では実施されなかった新たな対策が示されうることを述べた．

さらに，リスク表現におけるリスク源，事象，結果の関係性に対するリスク対応の考え方を導入し，情報システムの設計者の立場からの新たな技術的対策の観点を導出することで，本稿による失敗事例に基づく原因分析とその対策の導出による新たな失敗マネジメントの有用性を示した．

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，JIPDEC（オンライン），入手先 ⟨http://www.isms.jipdec.or.jp/isms/index.html⟩ （参照 2013-03-31）．

[2] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 27001:2005, Information technology – Security techniques-Information security management systems – Requirements (2005).

[3] 独立行政法人情報処理推進機構：組織内部者の不正行為によるインシデト調査調査報告書，独立行政法人情報処理推進機構（オンライン），入手先 ⟨http://www.ipa.go.jp/security/fy23/reports/insider/documents/insider_report.pdf⟩ （参照 2013-3-13）．

[4] 島　成佳：内部不正による情報セキュリティインシデントにおける内部者の意識と対策に関する分析と考察，CSS2012(3), pp.539–546 (2012).

[5] 畑村洋太郎：失敗学のすすめ，講談社 (2000).

[6] 濱口哲也：失敗学と創造学，日科技連出版社 (2009).

[7] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management (2005).

[8] 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).

[9] 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).
[10] 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).
[11] Insider Threat Center: The CERT Insider Threat Center, CERT (Online), available from ⟨http://www.cert.org/insider_threat/⟩ (accessed 2013-03-31).
[12] Andrew, P.M., Dawn, M.C. and Randall, F.T.: The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures, CERT (Online), available from ⟨http://www.cert.org/archive/pdf/08tr009.pdf⟩ (accessed 2013-03-31).
[13] Eileen, K., Dawn, C. and Andrew, M.: Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector, CERT (Online), available from ⟨http://www.cert.org/archive/pdf/insiderthreat_it2008.pdf⟩ (accessed 2013-03-31).
[14] 財団法人社会安全研究財団：情報セキュリティにおける人的脅威対策に関する調査研究報告書，財団法人社会安全研究財団（オンライン），入手先 ⟨http://www.syaanken.or.jp/wp-content/uploads/2012/05/cyber2203_01.pdf⟩（参照 2013-03-13）.
[15] 橘木俊詔，長谷部恭男，今田高俊，益永茂樹：リスク学入門 1 リスク学とは何か，岩波書店 (2007).
[16] 橘木俊詔：リスク学入門 2 経済からみたリスク，岩波書店 (2007).
[17] 長谷部恭男：リスク学入門 3 法律からみたリスク，岩波書店 (2007).
[18] 中西準子：環境リスク論，岩波書店 (1995).
[19] 村上洋一郎：安全学，青土社 (1998).
[20] 佐々木良一：IT リスクの考え方，岩波新書 (2008).
[21] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 31000:2009, Risk management – Principles and guidelines (2009).
[22] 独立行政法人情報処理推進機：情報セキュリティ教本，実教出版 (2010).
[23] 日本工業規格：情報技術—セキュリティ技術—情報通信技術セキュリティマネジメント—第 1 部：情報通信技術セキュリティマネジメントの概念及びモデル (2006).
[24] 佐藤亮太，高橋克巳，桑名栄二：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，CSS2011(3), pp.672–677 (2011).
[25] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC TR 13335:1997, Guidelines for the Management of IT Security (1997).
[26] International Organization for Standardization/International Electrotechnical Commission: ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management (2011).

付　　録

A.1 脅威と脆弱性の失敗学の類型化への対応付け

「情報セキュリティ」の項目において，赤色の項目は表 3 における脅威に相当する項目であり，D，A，E，N/A はそれぞれ「意図的脅威」，「偶発的脅威」，「環境的脅威」，「該当なし」を表す．さらに，青色の項目は表 3 における脆弱性に相当する項目である．

失敗学		
大分類	中分類	小分類
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かならずしも最初に考えるべきセキュリティ的な設計要因	材料の破壊	脆性破壊
		疲労破壊
		腐食
		応力腐食割れ
		高分子材料
	構造の破壊	バランス不良
		基礎不良
		座屈
	構造の振動	共振
		流体振動
		キャビテーション
	想定外の外力	衝撃
		強風
		異常摩擦
	バグ・セキュリティホール	
	内部関係者を利用しない攻撃	
	内部関係者を利用した攻撃	
技術的な要因だが，普通は副次的に考えているシステム/ソフトウェア使用時の設計要因	想定外の制約	特殊使用
		落下物・付着物
		波流
		腐食・動物
		想定蓄積
		システム環境故障
	火災・天災からの逃げ遅れ	油脂引火
		火災
		天災
	連鎖反応で拡大	脆弱構造
		フィードバック系暴走
		化学反応暴走
		細菌繁殖
		産業連関
	冗長系の非動作	フェイルセーフ不良
		待機系不良

情報セキュリティ	
脅威と脆弱性の例	分類
N/A	N/A
ソフトウェアの故障	D, A, E
ソフトウェアの公知の欠陥	D
NW構要素の技術的障害	A
トラフィックの過負荷	D, A
トラフィック分析	D
メッセージ経路変更	D
通信への侵入	D
悪意ある試行	D
保護されていない通信回線	通信
送信元および受信者の識別と認証の欠如	通信
悪意のあるソフトウェア	D, A, E
ソーシャルエンジニアリング	D
ユーザのエラー	D, A
ソフトウェアおよびハードウェアの正しくない使用	人事
静電荷	E
N/A	N/A
ほこり	E
N/A	N/A
障害	A
漏水	A
空調故障	D, A
ハードウェアの故障	A
記憶媒体の劣化	E
資源の飽用	D, A
電力の不安定	A, E
電磁波放射	D, A, E
回線の損傷	D, A, E
NWサービスの障害	D, A
N/A	N/A
火事	D, A
地震	E
台風	E
落雷	E
洪水	D, A, E
極端な温度および湿気	D, A, E
N/A	N/A

失敗学		
大分類	中分類	小分類
技術的な要因だが，人間や組織との関係が強い設計要因	作業で手を抜く	入力ミス
		保守作業ミス
		配管作業ミス
	設計で気を抜く	自動制御ミス
		流用設計
		だまし運転
		記録の欠如
		物理的な保護の欠如
技術ではどうしようもない組織的な要因	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
		不適切な情報管理
		不適切な要員管理
	悪意の産物	違法行為
		企画変更の不作為
		倫理問題
		テロ

情報セキュリティ	
脅威と脆弱性の例	分類
操作員のエラー	D, A, E
保守のエラー	D, A, E
送信エラー	A
不正確なパラメタ指定	ソフトウェア
アクセス権の誤った割り当て	ソフトウェア
不十分なパスワード管理	ソフトウェア
廃棄時の注意欠如	文書
記録媒体の不十分な保守・不適当な設置	ハードウェア
平文でのパスワード転送	通信
N/A	N/A
N/A	N/A
監査証跡の欠如	ソフトウェア
建物，ドアおよび窓の物理的保護の欠如	環境，施設
洪水の影響を受けやすい地域への配置	環境，施設
N/A	N/A
離席時にログアウトしない	ソフトウェア
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	環境，施設
文書化の欠如	ソフトウェア
有効な構成変更管理の欠如	ハードウェア
記録媒体の定期的な交換計画の欠如	ハードウェア
保護されていない保管	文書
管理されていないソフトウェアのOL	ソフトウェア
管理されていないコピーの作成	文書
要員の不在	人事
スタッフ不足	A
不十分なセキュリティ訓練	人事
セキュリティ意識の欠如	人事
故意の損害	D
盗難	D
盗聴	D
違法なソフトウェアの輸入・輸出	D
ソフトウェアの違法な使用	D, A, E
ユーザIDの偽り	D
不正なユーザによるNWへのアクセス	D
不正な方法でのNW設備の使用	D
不正なユーザによるソフトウェアの使用	D, A
不正な方法でのソフトウェアの使用	D, A, E
記憶媒体の不正使用	D
権限の乱用	D, A
N/A	N/A
不適切な採用手続き	人事
否認	D
争議行動	D, A
爆破行動	D, A
武器の使用	D, A

佐藤 亮太

2002 年大阪大学工学部応用自然科学科卒業．2004 年同大学大学院応用物理学専攻修士課程修了．同年日本電信電話株式会社入社．以来，情報セキュリティ，暗号システムの研究開発に従事．現在，日本電信電話株式会社技術企画部門所属．2011 年 FIT 論文賞受賞．電子情報通信学会会員．

間形 文彦 （正会員）

1992 年中央大学法学部法律学科卒業．同年日本電信電話株式会社入社．現在，NTT セキュアプラットフォーム研究所に所属．社会科学と情報工学の境界領域から情報セキュリティの研究に従事．日本セキュリティ・マネジメント学会，情報ネットワーク法学会各会員．技術士（情報工学）．

高橋 克巳 （正会員）

1988 年東京工業大学理学部卒業．同年日本電信電話（株）入社．2006 年東京大学情報理工学系研究科博士課程修了．博士（情報理工学）．NTT 研究所にて情報検索，データマイニング，位置情報処理，および情報セキュリティ，暗号，プライバシ，セキュリティ社会科学の研究に従事．本会理事．

桑名 栄二 （正会員）

1984 年電気通信大学大学院修了．同年日本電信電話公社入社．以来，ソフトウェア工学，インターネット，グループウェア，クラウド，情報セキュリティ等の研究開発に従事．2010 年 NTT 情報流通プラットフォーム研究所長，2012 年 NTT セキュアプラットフォーム研究所長，現在，NTT Innovation Institute Inc. 所属．博士（工学，筑波大学）．ACM 会員．