様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月１６日現在

機関番号：12102
研究種目：挑戦的萌芽研究
研究期間：2009～2011
課題番号：21650011
研究課題名（和文）　セキュリティシステムの危殆化リスク評価とシステム SLA の提案

研究課題名（英文）　Vulnerability Risk Assessment of Security Systems and Proposal for System SLA

研究代表者　岡本　栄司　（OKAMOTO EIJI）
筑波大学・システム情報系・教授
研究者番号：60242567

研究成果の概要（和文）：高度に発達した情報ネットワークにおいて、多くのセキュリティシステムが導入されているが、今までは攻撃等による危殆化に対する事前対策が主であった。しかし、実際にはどんな対策をとっても必ず危殆化するため、事後対策も同等に考慮した対策が必要となる。そこで、ネットワークにおける危殆化の確率とその被害を定量的に評価し、その評価を用いた危殆化リスクに強いセキュアネットワークシステムの構築し、それらに基づいた危殆化リスクの予測の試みを行った。その結果、SLA(Security Level Agreement)の形成に役立てることができるようになった。

研究成果の概要（英文）：A lot of security systems are introduced in recent highly advanced and sophisticated networks, but pre-active methods are used usually. However attacks are inevitable and it is not possible to stop all of them, so proactive methods are important. This is the idea of RISK. We presented a quantities approach for the effective and efficient assessment of risks related to information security, construct robust network systems using this assessment, and proposed a forecasting method of information security related incidents. SLA (Security Level Agreement) is possible using these methods.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,200,000	0	1,200,000
2010 年度	1,100,000	0	1,100,000
2011 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,200,000	270,000	3,470,000

研究分野：総合領域
科研費の分科・細目：情報学、計算機システム･ネットワーク
キーワード：ネットワークセキュリティ、リスク、脆弱性

１．研究開始当初の背景

現代社会は、高度に発達した情報システム基盤の上に成り立っており、非常に便利で快適な一方、マイナス面も併せ持っている。特に、プライバシ侵害や不正侵入などのセキュリティと、災害やテロなどが起きたときの被害が広範囲に及ぶという脆弱性が問題となっている。このため、これらに対する対策が採られてきたが、それは被害を０に近づけようという方針で立てられてきた。しかしながら、実際には被害発生を確率０にすることは事実上不可能であり、一般ユーザのサイドからは、想定外の被害が起きたらどうなるのかという不安が拭い切れない。

そこで、被害発生確率を０にすることにこだわらず、発生確率と、広い意味での損害額との兼ね合いを総合的に検討するリスク的考え方が重要視されてきている。このリスク的視点はあらゆる面に及んでおり、個人生活から企業活動にまで多岐にわたっている。とくに、環境・エネルギー・都市災害などではこのリスク管理が重視されている。

一方、情報セキュリティではリスク管理は行われていなかった。例えば暗号などは現実にはコンピュータの発達により解読の危機にさらされており、リスク管理は避けられないはずである。本研究により、正しいリスク評価に基づいたセキュリティレベル(SLA: Security Level Agreement)が提示されることになり、一般ユーザの安心感が醸成されることになる。

２．研究の目的

セキュリティを脅かす出来事が頻繁に起きる中で、情報セキュリティシステムの安全性･信頼性に関する意志決定が重要になりつつある。しかしながら、多くの企業では事業の効率性を重視するために、情報セキュリティ対策は後回しにして、費用も削ろうとする傾向にある。ところが、近年は政府やユーザから情報セキュリティに対する圧力が加わってきているため、効率性、経済性、安全･信頼性をトータルに考える必要が出てきている。その一つが情報セキュリティのマネジメントであり、正しくマネジメントするには情報セキュリティに関する定量化が求められる。そこで、情報セキュリティにおけるリスクマネジメントとアセスメントの確立を目指す。具体的には定量化に統計的手法と予測分析手法により、情報セキュリティインシデントの予測を行う。

これからのセキュリティシステムは、危殆化したときの対策を予め講じなくてはいけなくなる。従って、本研究で得られた成果は何らかの形で各セキュリティシステムに組み込まれることになろう。一般に被害はネットワークを通じて拡大するため、特にネットワーク上のセキュリティシステムが重要となる。セキュリティ関連製品は単独で用いられることはほとんどなく、他の製品に組み込まれる。従って、内部にかくれているが、全てのセキュリティ製品にかかわるため、波及効果は大きいと見られる。

一般ユーザの安心感は、正しいリスク評価とその正当な理解によってはじめて達成できるものである。そこで、その正当な理解を助けるために、上記のリスク評価支援ツールを基にしたシステム SLA(Security Level Agreement)を提唱しその普及をはかる。本来の SLA は Service Level Agreement であったが、我々は Security の意味で用い、利用者と提供者間のセキュリティレベルの合意形成を目指すものである。

３．研究の方法

高度に発達した情報ネットワークにおいて、多くのセキュリティシステムが導入されているが、今までは攻撃等による危殆化に対する事前対策が主であった。しかし、実際にはどんな対策をとっても必ず危殆化するため、事後対策も同等に考慮した対策が必要となる。そこで、

(1) ネットワークにおける危殆化の確率とその被害を定量的に評価
(2) その評価を用いた、危殆化リスクに強いセキュアネットワークシステムの構築
(3) それらに基づいた、危殆化リスクの予測の試み

という方法により研究を行ってきた。その結果、次に示すように、ネットワーク強度評価ツールを構築し、実際のネットワークに適用してセキュリティシステムのリスク評価を行ない、有効性を確認できた。その結果、SLA の実現に役立った。

４．研究の成果

(1) 危殆化リスクの定量化

① 初期設置

（ｉ）情報セキュリティポリシーの初期設置

組織において、情報セキュリティリスク評価と予測のために、最初にセキュリティポリシーをどう設定するかを検討した。まず従来の IT システムへの攻撃に対する経済的なセキュリティポリシー対策を調査し、現状の標準やガイドラインがベストプラクティスになり得るか、あるいは侵入などの脅威モデル構築の知識として有効かを定性的に検討した。

（ⅱ）リスク評価と予測の定量的手法の初期設置

情報セキュリティの定量的手法の設置/配置に用いることを念頭に、情報セキュリティリスクの定量的評価と情報セキュリティインシデントの予測のために IT システムへの脅威の活動量を示す統計的データの収集を行った。

一般に攻撃源は、脅威を与える一連の攻撃を実行するが、攻撃源から潜在的脆弱システムへの攻撃による損失評価を行うことになる。これを分類化して、IT システムの変更に対策も追随しやすくした。これは同質のアタックをひとまとめにして対策するのに有効である。

損失については、経済的にはリスクは損失の期待値として扱われる。従って、損失がなければリスクはない。IT の立場から言えば、いくら損失がなくてもセキュリティポリシーの欠陥あるいは潜在的損害の可能性があ

ればリスクありと判断する。組織的セキュリティ対策がなくても、運良く外的要因でその時は現れなかっただけかも知れない。そこで、ここでは生起分布の変位値を元に経済的要素を取り除いて定量化を図った。

情報セキュリティインシデントは次の2つに分類される。曖昧さ無し検知可能な場合と曖昧さ無しには検知不可能な場合である。曖昧さ無しには検知できないとなると、定量化と予測が不可能となるので、定性的にしか扱えなくなる。

ここでは曖昧さ無し検知可能な場合を取扱う。この結果を曖昧さ無しには検知不可能な場合に適用することもできなくはないが、インシデント予測やリスク評価が不正確になる。

② 情報セキュリティリスク評価

(ⅰ) 従来法

情報セキュリティリスク評価手法を与え、その応用例を示す。そのために、まず従来手法を調査し、それらの問題点を示す。

(ⅱ) 問題点

1) トータルリスクマネジメントへの適用における問題点

評価結果をトータルリスクマネジメントに適用するためには、トータルなので広範囲に受理される出力基準としなければならない。ここでは2つの基準を用いる。一つは年損失期待値(ALE)であり、もう一つはリスク値 VaR である。

ALE の計算には情報セキュリティリスクでは定義しにくいパラメータを用いるが、VaR にはそのようなことはない。一方、VaR の入力は統計的データから計算できる。ただし、インシデント頻度と損失についての累積分布関数を計算するには、付加的な新たな統計的処理を必要とする。

2) 評価対象の問題点

リスク評価における入力データの値に関して業界に統一的な基準がない。従って、幾つかのアプローチを適用する必要が出てくる。そこで、リスク評価手法をマクロ的アプローチとミクロ的アプローチにクラス分けした。マクロ的アプローチは従来起こった損失の解析から行うため、従来データの不足や未知のことに対処できず、事後対策となる。

他方、ミクロ対策は各リスクの脅威分析や脆弱性評価の予測から始める。それは潜在的危険イベントのリスト生成から始まる。

ここでは、これらのアプローチを融合する。全ての生起損失はインシデントに起因するため、統計的データは脅威源と脅威型により分類できる。同時にこの脅威による潜在的危険事象に対しては、設置対策によって防がれた各インシデントに対する経済的損失軽減量を予測する必要がある。つまり、本提案方式を IT システムに適用することにより、実際に生じた損失量と防げた損失量をもとめ、本提案方式の効果を計る。それを日単位で求めた Daily Risk と年単位の Annual Risk で表す。これを現在の対策あるいは将来の対策後の影響から差し引くと、その脅威に対する当該対策の正味の効果がわかる。

経済的に計れない潜在的危険事象に対しては、リスク対策は似たように評価されるが、損失時刻系列直接よりもその原因となったインシデント全体の時刻系列を用いることになる。

3) 累積分布関数評価の問題点

VaR を計算するには、損失あるいはインシデント数の累積分布関数を評価する必要がある。

情報セキュリティインシデントによる損失に関連した均質統計データの収集に際しての問題は、IT システムにおける不均一生、継続する過剰変動である。これは IT 業界ではよく起こることである。もし、情報セキュリティインシデントと関連する潜在的危険事象の因果関係がわかると、リスク評価に関する潜在的危険事象の個数から間接的にインシデントの発生回数を評価することになる。しかし、そのような因果関係導出ができない場合は、次善策として脆弱性のコンフィギュレーションプロファイルを用いる。

脆弱性コンフィギュレーションプロファイルというのは予め決められた脆弱性のセットである。

一般に、コンフィギュレーションプロファイルは IT インフラをオーメーション化したビジネスタスクのソリューションを簡単化し、ビジネスタスク自体の数も減らすためにある。こうすることにより、多くのビジネスユーザの要求に応えられるような、統一的で決まった形の応用が可能となるからである。これがコンフィギュレーションプロファイルであって、ハードウェアとソフトウェア両方のイメージがあり得る。

これをリスク評価に用いると次のようになる。脆弱性セットをコンフィギュレーションプロファイルとみなす。そして、多くのコンピュータに起こったセキュリティインシデントは、この脆弱性コンフィギュレーションプロファイルに関連した脆弱性分布と同じ分布を持つ乱数変数と、当該組織に固有の脅威全体のセットにおける脅威の分布と同じ分布を持つ乱数変数との多変数確率関数となる。

従って、同じコンフィギュレーションプロファイルの異なるサンプルから収集した統計量は、同一確率パラメータを持つ多重実験の結果を表現していると見なせる。与えられた資産に対するリスクは2つの確率と定数としての資産価値の積で定義されてタイプ化されるので(従って同じタイプならば資産価

値も同じと見なされるので)、脅威分布は組織全体で同一であり、脆弱性は対応コンフィギュレーションプロファイルで一定値となり、収集された統計データは均質となる。よって、セキュリティインシデントと損失の累積分布関数の近似式として利用できるようになる。

4) 損失時刻系列の安定性の問題

本研究では安定性のチェック法とトラブル時に時系列を安定状態へ変換する方法を示し、変換とデータ解析法を示した。

(iii) リスク評価法の提案

ここでは本研究の中心となるリスクの累積確率分布関数の予測に用いられる統計的ブロック方式と情報セキュリティインシデントによる損失の評価法を示す。

ところで、通常そのような方式は関連する統計データを多く集める必要があるが、セキュリティ実施者が得られるリスク関連統計データの量は実はそれほど多くはない。それは攻撃を受けている対象システムの統計データは集められないからである。

そこでここでは少ないデータサンプルでもかなり正確に見積もれる統計手法を提案する。それは次の 2 つ評価結果を出力する。

・Daily Risk

・Annual Risk

これらの導出のために、VaR (Value at Risk)と呼ばれるよく知られた金融リスク評価と Rosenblatt-Parzen Kernel 密度評価手法を用いる。これらは次のように書ける。

・ Daily Risk=$VaR^{Daily\ Loss}(a)=CDF^{Daily\ Loss}(a)=q_a^{Daily\ Loss}$

・Annual Risk=$VaR^{Annual\ Loss}(a)=CDF^{Annual\ Loss}(a)$

ここで

$VaR^{Annal\ Loss}(a)=\inf\{CDF^{Loss}(L)>a\}$

である。

従って、Daily Loss を計算するためには Epanechnikov Kernel を持つ Rosenblatt-Parzen Kernel 密度評価を、収集した Daily Loss 時系列に適用する必要がある。

情報セキュリティの仕様によっては、Daily Loss とは同じようにして Annual Loss を計算できないことがあるので、ここでは中央極限定理を用いた近似式を利用することとした。さらに統計データが少ない場合は Annual Loss の上界のみ導いた。

ここで Daily Loss 時間系列の i 次相関係数を ρ_i とする。Annual Risk を下記に示すが、リスクを計算する際、過剰評価より過小評価が問題となるので、365 観測より少ない場合は、欠けたところは $\rho_i=1$ とする。すると Annual Risk は次式で与えられる。

・$Annual\ Risk=VaR^{Annual\ Loss}(a)$

$=CDF^{Annual\ Loss}(a)$

$=q_a^{Annual\ Loss}=\Phi(a)\times(Variance(\Sigma_{i=1}Daily\ Loss_i))^{1/2}$

$=\Phi(a)\times(n\sigma^2+2(n-1)\rho_1\sigma^2+\cdots$

$+2(n-(n-1))\rho_{n-1}\sigma^2))^{1/2}$

ここで σ^2 は分散であり、Φ はガウス分布である。

本研究では、この結果を、よく知られた Net Present Value (NPV)指標に基づいたセキュリティ投資の実施の利益評価に適用する方法を示した。

(iv) ケーススタディ

実際の IT システムにおける一つのリスクに上記結果を適用した。ここで、提示の簡単化のために、生起した情報セキュリティインシデントの全てがわかり、関連損失もわかる場合を取り上げた。その結果、損失は一意的に求められた。

③ 情報セキュリティインシデントの予測

(i) 提案方式の適用

個々で用いる統計データは、ある企業において CEO (Chief Executive Officer)の許可を得て連続した 199 日間でとったものである。この例で用いられたインシデントは当該会社へのスパムメール到着時刻系列である。スパムメールか否かは受け取る人によって異なる。従って、調査協力者がスパムフィルタをはずして IT スタッフに毎日のスパムメール数を報告するようにした。これにより、日々のインシデント生起数系列が得られる。

IT システムの構成上からは、外部に繋がっているメールサーバ(External Mail Server)と内部同士でのやりとりを司るメールサーバ(Enterprise Resource Planning)の 2 種類から収集している。この企業の特徴として、メールは内部間の方が外部とのやりとりより多い。

その時系列統計データをもとに次のような処理を行う。

1) インシデントから損失(ロス)への変換

スパムメール自体から直接企業資産にダメージを与えるわけではないので、社員のスパムメール処理にかかる時間がロスなる。処理に 10 秒かかるとして、ローディング的にはスパムメール一つは 5 円程度のロスとなる。こうすると Amount of Incidents の日毎曲線と Daily Loss は同じ形状となるが、一般にはこんな単純ではないので同じとはならない。

2) データ解析

Daily Loss 時系列は安定系列ではないが、New Stationary Data へのある変換を施すことにより、安定系列となる。

3) Daily Loss の分布関数予測

安定系列に変換することにより、我々の提案した方式を適用して密度関数の評価が可能となる。

4) Daily Risk と Annual Risk の推定

Rankit-Cleveland 変位値推定法を適用することにより、1 日あたりの Daily Loss が具

体的に 2.8023 と判明するので、ある日 d の Daily Risk は、多少の計算の後
Daily Risk=4.7801+(-0.007723)(d-1)
となる。
従って、スパムメールに対するこの組織の Annual Risk は、95%の信頼度で 60000 円ぐらいである。
これらは一計算例であり、必ずしも実態を反映しているとは限らないことに注意を要する。
5) スパムメール対策のコスト分析
以上の結果からスパムメール対策にどの程度投資すればいいかがわかる。すなわち、この部門ではスパムメールのリスクは年 6 万円程度であり、対策費用もその程度にするのが妥当である。
④ 危殆化リスクの予測システム
危殆化リスクの予測システムはシステム SLA の根幹をなす重要なものであるが、回帰的手法を用いて将来の危殆化リスクを予測するシステムを開発し、実際のデータで検証した。

(2) セキュアネットワークの構築
次に、ネットワーク脆弱性評価のために、現実のネットワーク情報を自動取得して可視化、脆弱性分析するステムを開発した。
それを用いてネットワークのリスク評価支援ツールを構築し、現実の情報ネットワークに適用してマルウェア侵入リスクの脆弱性評価を行った。
マルウェア侵入リスクの脆弱性評価に基づいて、危殆化に強いセキュリティシステムを構築した。具体的にはパケットマーキングを用いる方法を提案し、マルウェア等の不正アクセスリスクを回避できるネットワークシステム構成法を提案した。

以上、情報セキュリティに関するリスクの定量アセスメント手法を開発し、情報セキュリティインシデントの予測の予測を行った。具体的にはスパムメールに関する定量的予測を行い、現実データと合うことを示した。
開発したシステムは SLA ツールとして、有用であり、セキュリティレベルの合意に役に立つ。この結果、企業や政府、地方公共団体における情報セキュリティに関連した意志決定を行うことができる。また、銀行、証券、監査などにも役に立つ。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 12 件）
①Sk. Md. Mizanur Rahman, M. Anwar Hossain, Hussein Mouftah, Abdulmotaleb El Saddik and Eiji Okamoto; Chaos-cryptography based privacy preservation technique for video surveillance, Special Issue on Privacy-aware multimedia surveillance systems, Multmedia Systems, Springer, Vol. 18, No.2, pp.145-155, 査読有, 2012, http://dx.doi.org/10.1007/s00530-011-0246-9
②秋山浩岐、満保雅浩、岡本栄司；検索クエリ中のワイルドカードを秘匿する隠れベクトル暗号システム、情報処理学会論文誌、Vol.52, No. 9, pp.2662-2673, 査読有, 2011 年 8 月
③岡田雅之、金岡晃、勝野恭治、岡本栄司；確率的パケットマーキングにおける最適マーキング確率の推定、情報処理学会論文誌, Vol.52, No. 9, pp.2718-2728, 査読有, 2011 年 8 月
④原田敏樹, 金岡晃, 加藤雅彦, 岡本栄司；ネットワークシステムにおける脆弱性影響の測定手法とシステム実装、情報処理学会論文誌, Vol.52, No. 9, pp.2613-2623, 査読有, 2011 年 8 月
⑤A. Romanov, H. Tsubaki and E. Okamoto; An approach to perform quantitative information security risk assessment in IT landscape, 情報処理学会論文誌, 査読有, 51 巻 9 号 pp.1726-1749, 2010
⑥金岡晃, 原田敏樹, 加藤雅彦, 勝野恭治, 岡本栄司, ″安全なネットワークシステム設計のためのマルチレイヤネットワークモデルの提案と応用″, 情報処理学会論文誌, Vol.51, No.9, pp.1726-1735, 査読有, 2010
⑦A. Romanov and E. Okamoto; Forecasting of information security related incidents: Amount of spam messages as a case study, 電子情報通信学会論文誌, 査読有, E93-B 巻 6 号, pp.1411-1421, 2010
⑧猪俣敦夫、岡本栄司；我々をとりまく情報社会と暗号危殆化のかかわり、情報処理学会 50 周年記念「情報処理技術の未来地図」、査読有, 51 巻、5 号、pp.528、2010
⑨金岡 晃、勝野恭治、岡本栄司；メーリングリストを考慮したマスメール型ワームの感染数理モデル、情報処理学会論文誌、Vol.51, No.3, pp.682-690, 査読有, 2010 年 3 月

〔学会発表〕（計 25 件）
①金岡 晃、岡田雅之、岡本栄司；確率的パケットマーキング手法の実用化検討、CSS2011、2011 年 10 月 19-21 日、 朱鷺メッセ(新潟県)
②日暮一太、金岡 晃、加藤雅彦、岡本栄司；マルチレイヤのネットワークトポロジ抽出

手法、第 10 回情報科学技術フォーラム (FIT2011)、電子情報通信学会＆情報処理学会、2011 年 9 月 7-9 日、函館大学（北海道）
③ A. Moreno, E. Okamoto; BlueSnarf revisited: OBEX FTP services directory traversal, Workshop on Wireless Cooperative Network Security (WCNS 2011), 2011.5.9-13, Valencia, Spain
④Masayuki Okada, Akira Kanaoka, Yasuharu Katsuno, Eiji Okamoto; 32-bit AS Number Based IP Traceback, Fifth International Workshop on Advances in Information Security (WAIS-2011), Seoul, Korea , June 30 - July 2. 2011
⑤Xun Yi and Eiji Okamoto; Key agreement for large-scale dynamic peer group, ADPC2010 (Advances in Distributed and Parallel Computing), 2010 Nov.1st-2nd, Mandarin Orchard Hotel, Singapore
⑥金岡 晃、加藤雅彦、岡本栄司；Web 感染型マルウェアリスク評価を可能とするネットワークトポロジ分析、電子情報通信学会 ICSS 研究会、2010 年 11 月 5 日，広島市立大学（広島県）
⑦ Raylin Tso, Xun Yi, Tadahiko Ito, Takeshi Okamoto and Eiji Okamoto; Design and analysis of “Flexible” k-out-of-n Signatures, ATC2010 (The 7th International Conference on Autonomic and Trusted Computing), Xi¡an, China, 26-29 October, 2010
⑧ Anton Romanov and Eiji Okamoto; A quantitative approach to access information security related risks, 4th International Conference on Risks and Security of Internet and Systems (CRISIS2009) , Toulouse, France, October 19-22, 2009
⑨ Anton Romanov and Eiji Okamoto; An Approach for designing of enterprise IT landscapes to perform quantitative information security risk assessment, ICETE/SECRYPT2009, July7-10, Milan, Italy
⑩ Anton Romanov and Eiji Okamoto; A Framework for Building and Managing Secured ERP Landscape, WORLDCOMP'09/SAM'09, LasVegas, Nevada, USA, July 13-16, 2009
⑪Akira Kanaoka, Masahito Kato, Nobukatsu Todo and Eiji Okamoto; Extraction of Parameters from Well Managed Networked System in Access Control, The Fourth International Conference on Internet Monitoring and Protection (ICIMP 2009), May 24-28, 2009 - Venice/Mestre, Italy

６．研究組織
(1)研究代表者
岡本 栄司（OKAMOTO EIJI）
筑波大学・システム情報系･教授
研究者番号：60242567

(2)研究分担者
金岡 晃（KANAOKA AKIRA）
筑波大学・システム情報系･助教
研究者番号：00455924

(3)連携研究者
（ ）

研究者番号：