ＩＤＣ(インターネット・データ・センタ)の
セキュリティ向上を目指して

富士通エフ・アイ・ピー株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

深　澤　　哲

1999 年　富士通エフ・アイ・ピー（株）入社
　　アウトソーシングサービス部
　　見積業務担当
2001 年　アウトソーシングサービス部
　　IDC 業務担当
2002 年　現在 上に同じ

■ 論文要旨 ■

筆者は，ＩＤＣの共用ＤＮＳ及びメールサーバの運用と管理という業務に従事しており，担当ＳＥという立場であるが，一方でセンタ管理者が行うプロジェクトの管理/監査の業務にも携わっている．例えば，センタ管理者の立場でセキュリティ監査を行ったり，プロジェクトを管理する社内ツールの作成を行うといったことである．

ＩＤＣでは，インターネットを利用するという業務上，セキュリティ運用は欠かすことができない．本論文は，実際にセキュリティ対応を行っている担当ＳＥという側面とプロジェクトを管理/監査するセンタ管理者という側面の両面からセキュリティ運用の現状を分析し，また改善への取り組みについて論ずる．

■ 論文目次 ■

■ 図表一覧 ■

１．はじめに

１．１　当社概要

当社は，２００１年４月よりＩＤＣ(インターネット・データ・センタ）としてサービスを開始し，多くのユーザに利用されている．現在では，ユーザ数は飛躍的に増加してきており，前年度に比べて倍以上の伸びを示している．

１．２　IDC 業務の特徴

ＩＤＣの業務では，Ｗｅｂやメールサービスを始めとしたインターネットを利用するサービスというのが特徴である．インターネットを利用しているという性質上，不特定多数のクラッカーからの脅威にさらされており，業務担当者は常にセキュリティについて気を配っておく必要がある．また，考慮しなければならない事象は多岐に渡っており，盗聴や不正アクセス等による情報漏洩は深刻な問題である．

２．セキュリティ運用の現状

ＩＤＣの業務を運営していくうえでセキュリティ運用は，欠かすことができない．その主な内容は以下の通りである．

・セキュリティ情報の収集(担当 SE)
・アプリケーションのバージョンアップ/パッチの適用(担当 SE)
・プロジェクト管理(担当 SE)
・セキュリティ監査(センタ管理者)

これらの運用について担当ＳＥとセンタ管理者の観点から現状の問題点について考察する．

２．１　担当ＳＥからの観点

ＩＤＣで行われているセキュリティ運用は，各プロジェクトごとに業務担当者が対応するというものである．例えば，担当するプロジェクトごとにセキュリティ情報を収集しながらインストールしているソフトウェアについて問題の有無を検討し，必要であればバージョンアップやパッチを適用していくというものである．

しかし，随時更新されていくセキュリティ情報を各自で収集し，必要な対策を講じるというのは担当ＳＥにかかる負担も大きく，重大なセキュリティ情報を見逃すということにもなりかねない．また，個々のプロジェクトごとに対策を講じていると，情報の収集だけで多大な時間がかかってしまうことになる．

２．２　センタ管理者からの観点

センタ管理者はセキュリティ運用の一環として各プロジェクトのセキュリティ監査を行っている．しかし，各プロジェクトの情報は担当ＳＥで管理しているため，監査を行うためには，まず担当ＳＥから情報を収集することから始める必要があり，手間が掛かっているというのが現状である．

２．３　課題

以上のような現状から問題点をまとめると以下のようになる．

現状の課題

・セキュリティ情報の収集に多大な時間がかかる(担当 SE)
・担当ＳＥごとにセキュリティ対応にばらつきがある(担当 SE)
・プロジェクト情報を収集するのに時間がかかる(センタ管理者)
・セキュリティへの対応状況が把握できていない(センタ管理者)

つまり，担当ＳＥの観点からも管理者の観点からも，セキュリティ運用の面で効果的な対策がとられていないというのが現状である．

３．セキュリティ運用の改善に向けて

以上のような課題に対して，ＩＤＣでは現状を改善するため以下のような案を考えた．

改善案

・セキュリティ情報をセンタで一括収集する
・収集した情報はデータベース化し，SE が参照できるようにする
・分散しているプロジェクト情報を統合し，一括管理できるようにする
・セキュリティ情報とプロジェクト情報を連携し，問題のあるプロジェクトの抽出を行う

セキュリティ情報の一括収集は，今まで担当ＳＥが独自におこなってきたセキュリティ情報の収集を，センタで一括収集することでＳＥの負荷を軽減させるということが目的である．そのため，収集したセキュリティ情報はデータベース化し，担当ＳＥが自由に参照できることにする．

また，分散しているプロジェクト情報を一括管理することで，センタ管理者が容易に管理できるようにする．その際に考慮することは，セキュリティ情報と連携させるということである．具体的には，使用しているＯＳ，アプリケーションとバージョン情報を管理し，その情報からセキュリティ情報に該当するプロジェクトを抽出できるようにする．

以上のような改善案を実現するため，ＩＤＣではセキュリティ管理データベース(以後セキュリティＤＢ)を構築することになった．

４．セキュリティＤＢの構築

４．１　セキュリティＤＢの設計

このデータベースは担当ＳＥにも公開するということを考慮しているため，ローカルのツールではなくＷｅｂアプリケーションとして構築することにした．管理する情報はプロジェクト情報とセキュリティ情報であるが，主な項目は以下の通りである．

プロジェクト情報

・業務情報（顧客名，サービス内容，設置場所，担当部署，担当ＳＥ 等）
・サーバ情報（機種，ＯＳ，ドメイン，ＩＰアドレス 等）
・ソフト情報（使用ソフト，バージョン，適用パッチ，パッチ適用日 等）

セキュリティ情報

・脆弱性についての概要
・影響と対応策
・該当するＯＳ，アプリケーション，バージョン
・関連リンク（情報元，パッチ提供元 等）

４．２　公開する情報の制限

セキュリティＤＢを構築するにあたって最も注意を払わなければならないことは，公開する情報をコントロールするということである．つまり，公開する情報と公開しない情報をアクセスしてくるユーザ毎に区別するということである．

セキュリティＤＢは担当ＳＥにも公開するということを目的としているが，すべての情報を公開するというわけではない．例えば，担当ＳＥであればアクセスできる情報は，自分の担当するプロジェクト情報だけに制限し，他のプロジェクトの情報は見えないようにする(**図１**)．これは顧客情報の流出を防ぐためである．一方，センタ管理者であれば，全てのプロジェクト情報が参照できるということにする．

但し，セキュリティ情報については，担当ＳＥやセンタ管理者といった区別はなく，すべての人が参照できるということにする．

以上のことを考慮すると，セキュリティＤＢに求められる条件は以下の通りである．

求められる条件

・プロジェクト情報は担当者(顧客担当責任者，担当ＳＥ)のみに公開
・センタ管理者には全ての情報を公開
・セキュリティ情報は利用者全てに公開

図１　アクセスコントロールについて

担当 SE は自分の担当するプロジェクト情報にしかアクセスできない

４．３　セキュリティへの配慮

近年，Ｗｅｂアプリケーションにおける情報漏洩についてマスコミにも頻繁に取り上げられているが，セキュリティＤＢはＷｅｂアプリケーションとして構築するため，このような情報漏洩についても考慮する必要がある．

Ｗｅｂアプリケーションにおける情報漏洩についてその原因を調査した結果，主な要因には以下のことが挙げられる．

情報漏洩の主な要因

・クロスサイトスクリプトの脆弱性
・Cookie 情報の漏洩
・アクセス権の設定ミス

クロスサイトスクリプトの問題は，公表（２０００年２月）されてからかなりの期間が経過しているが，今なお多くのＷｅｂサイトがこの問題を抱えている．この問題は任意のスクリプトが実行可能状態になっていることにあるが，その要因にはＷｅｂアプリケーションの問題とＷｅｂアプリケーションサーバの問題の両方のケースが考えられる（**図２，３**）．しかし，多くの場合，エスケープ処理を怠っているなど開発側の対応漏れが原因であることが多い．

図２　エスケープ処理を怠ったアプリケーションの例
フォームの入力値チェックを怠っているため，スクリプトが実行されている

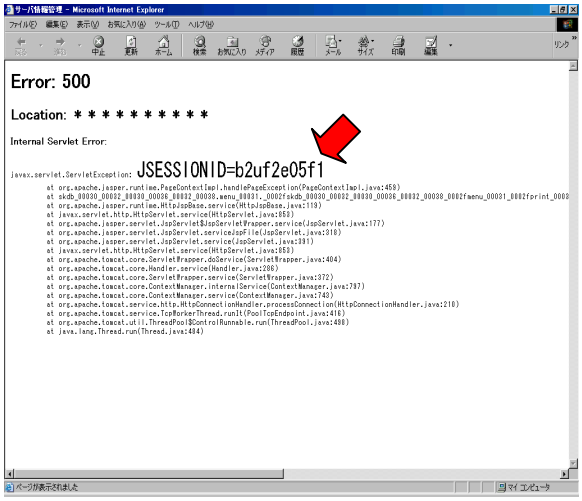

図３　Java Servlet コンテナに存在するクロスサイトスクリプトの脆弱性
任意のスクリプトが実行可能状態にあり，Cookie情報が漏洩している

Cookie 情報の漏洩については，クロスサイトスクリプトの脆弱性とも関連しているが，そもそも個人情報を Cookie に書き込むこと自体に問題がある．Cookie 情報の漏洩はクロスサイトスクリプトの脆弱性だけでなく，他にも多くの事例が公表されており，Cookie の利用は最小限にとどめておくべきである．

アクセス権の設定ミスについては，本来，制限すべきファイルを公開ディレクトリに配置し，かつアクセス制限をかけていないことが原因である．扱う情報に機密性がある場合（例えば個人情報など）は，特に気を遣うべきであり，公開する情報とは明確に区分しなければならない．

以上のような要因に対する主な対策は以下のとおりである．

主な対策

・エスケープ処理
・Cookie 利用の制限(セッションＩＤのみ)
・Ｗｅｂアプリケーションサーバのバージョンアップ

エスケープ処理は，フォームなどから入力された特定の文字(＜ ＞ ＆ ” ’)を変換するという処理である．この処理によって，本来，文字列として扱われる情報をスクリプトとして処理してしまうということを防ぐことができる．

Cookie については，使用するのはセッションＩＤのみとし，個人情報を含むその他の情報は一切利用しないようにする．また，その際セッションＩＤが推測できないものであることも重要である．

Ｗｅｂアプリケーションサーバについてはセキュリティ情報をチェックし，使用しているＷｅｂアプリケーションサーバに脆弱性がでていないかチェックを行う．脆弱性を含んでいるバージョンを使用している場合は，バージョンアップを行うか，場合によっては他

のＷｅｂアプリケーションサーバに切替える必要がある．

５．セキュリティＤＢの運用

５．１　機能

セキュリティＤＢの主な機能は以下の通りである．

・プロジェクト情報の参照/検索
・セキュリティ情報の参照/検索
・セキュリティ上問題のあるプロジェクトの抽出

プロジェクト情報は担当ＳＥが登録作業を行い，センタ管理者が一括管理している．登録作業はセキュリティ対応のためバージョンアップを行った際など，担当ＳＥによって随時行われている．また，セキュリティ情報はセンタ管理者が毎日情報収集を行い，必要な情報について登録作業を行っている．

５．２　運用

セキュリティＤＢは，現在，セキュリティ管理者によって運用されている(**図４**)が，その運用手順は以下のようになっている．

運用手順
１．セキュリティ情報を収集し，セキュリティＤＢに登録する(管理者)
２．プロジェクト情報とマッチングし，該当プロジェクトを検出(管理者)
３．該当プロジェクトの担当ＳＥにメールで情報を発信する(管理者)
４．セキュリティ情報を参照し，必要な対策を行う(担当ＳＥ)
５．セキュリティＤＢに対策内容を登録する(担当ＳＥ)
管理者はすべてのプロジェクトのセキュリティ対応が完了するまで，以上の手順を繰り返し行っている．

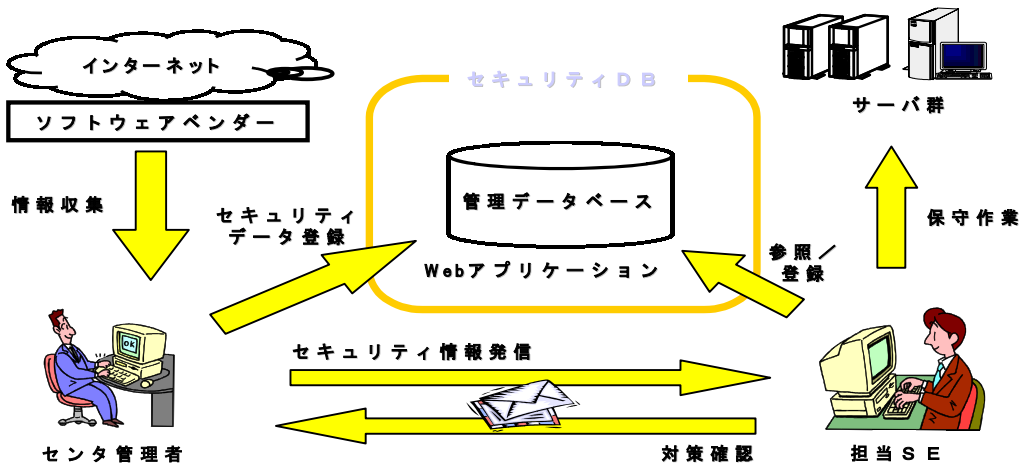

図４　IDC のセキュリティ運用

６．導入効果

６．１　担当ＳＥからの観点

担当ＳＥの観点からみると，セキュリティ情報はセンタで一括収集されているため，従来のように個人個人でＷｅｂサイトを見てまわる必要がなくなり，効率よく情報を把握することができるようになっている．また，プロジェクト管理とセキュリティ管理をセンタ管理者に一任することで，担当ＳＥはセキュリティ対応のみに専念することができるようになっている．

６．２　センタ管理者からの観点

センタ管理者の観点からは，分散されていたプロジェクト情報を統一化でき，管理が容易になるとともに，セキュリティ上問題のあるプロジェクトの抽出が可能となっている．また，セキュリティの対応状況を把握できるようになり，未対応のプロジェクトに対して対応を迅速に行うことができるようになっている．

図５はセキュリティＤＢのプロジェクト情報を表示した画面である．

業務情報やサーバの機種ＯＳ，ソフトウェア情報を始めレイアウト情報なども登録されている．

図５　プロジェクト情報

図６はセキュリティ情報を表示した画面である．セキュリティ情報には脆弱性の概要と影響，対処方法などが登録されている．

また，セキュリティ情報は対象となるＯＳやアプリケーションによって検索することが可能である．

図６　セキュリティ情報

６．３　情報発信の実績

セキュリティ情報発信の実績を**表１**に挙げる．この情報は該当するプロジェクトの担当者にメールで発信されており，担当ＳＥにて対応を行っている．

表１　主なセキュリティ情報の発信実績

■ 主な情報発信内容

2002/4	IIS※1 の脆弱性(4月17日)	5ユーザ / 8台 該当
2002/5	SystemWalker※2 のセキュリティ問題 (5月14日)	10ユーザ / 26台 該当
2002/6	Apache※3 のセキュリティホール (6月18日)	14ユーザ / 37台 該当
2002/6	proftpd※4 にDos攻撃を受ける問題 (6月27日)	7ユーザ / 11台 該当

※1 IIS:マイクロソフトのWWWサーバ　※2 SystemWalker:富士通の総合運用管理ツール
※3 Apache:UNIX,Winodws系OSのWWWサーバ　※4 proftpd:UNIX系OSのFTPデーモン

従来の運用では，担当ＳＥはセキュリティ情報の収集から始めて対応策の検討まで行う必要があったが，現在の運用では，対応策も含めてセンタで一括して情報を発信しているため，ほとんどのケースで即日対応ができるようになっている．

７．まとめ

７．１　今後の展開

ＩＤＣで運用しているセキュリティＤＢでは，管理者から担当ＳＥに向けての情報発信が主であるが，現在，ＳＥが他のプロジェクトのＳＥへ情報を発信できるような仕組みを構築しているところである．これはＳＥ同士での情報交換の場を設けることで，例えば，パッチをあてたときの不具合情報やその解決策といった情報を共有することが目的である．

７．２　おわりに

セキュリティの問題はシステムの初期構築だけで終了するものではなく，日々向き合っていかなければならない問題である．そのためＩＤＣで行ってきたセキュリティ管理は，盗聴や不正アクセスといったインターネット上の脅威を防止するというだけでなく，業務担当者への負担軽減も目的としたものである．

今日，インターネットに潜む脅威は確実に身近なものになりつつある．そのとき重要なことは身を守るための方法を知っていることであると考え，セキュリティ管理と情報発信を行ってきた．これからもＩＤＣ全体を通してセキュリティレベルが向上するよう，セキュリティの運用管理を行っていきたいと思う．