M-012

コンピュータセキュリティインシデントとその対応支援システム

Computer security incident and A Incident Handling System

梅澤昭生† 横地裕† 田中貴志† 門脇正†
Akio Umezawa Yutaka Yokochi Takashi Tanaka Tadashi Kadowaki

1．はじめに

近年のインターネットの急速な普及とブロードバンド化の進展は,ユーザーが急拡大するとともに,あらゆる活動を構成する不可欠な要素となっている.一方で 2004 年に発生した Sasser ワームのようなコンピュータウィルスやネットワークの機能不全,社会的混乱等を狙ったコンピュータセキュリティインシデントが多発し,対応が求められる報告件数が急増している．これらインシデントの状況を早期に把握して対応を行うためには，インシデントの情報交換が有効であり,システマチックに対処する手段を整備する必要がある．今回,インシデントと付随するその他のデータを交換する方式を検討し,インシデント情報交換システムを試作した.

2．コンピュータセキュリティインシデントの傾向と課題

過去 1988 年にインターネットワームというコンピュータセキュリティインシデントが発生した．その際の対応は,各インシデント対応機関が個別に対応し,機関同士の調整がとれていないものであったため,各関係機関はこのインシデントによって多大な被害をこうむった．このように特に広域に影響を及ぼすインシデントへの対応の場合は各機関が独自に対応をすると,調査や研究などが重複し非常に非効率的であるため,より多くの被害を被ることとなる．また大規模なインターネットワームなどの被害は国境を越えて発生するため,各国における迅速な状況把握が必須である．このようなインシデントへの対応には,各機関の対応状況を取りまとめ,情報の共有を取りまとめる中央機関が必要である．その中央機関においては,インシデント解決のためや情報交換のためにコミュニケーションをとる際に言語・時差・国際基準や協定に関する問題に直面する．この問題を解決することでインシデントへの迅速な対応や正確な情報の共有が出来る．これらのことから,セキュリティ情報交換フォーマットの策定が必要であり,近年では,各標準化団体においてセキュリティ情報の統一された標準フォーマットが標準化活動中である．現在,国際標準となっているフォーマットがないため,セキュリティ情報の交換を行う際には国や産業ドメイン,組織をまたいでの情報交換においては,その作業が困難である．セキュリティに関連する情報を,標準化された共通言語,及び共通フォーマットでやり取りすることで,

① 常時共通の認識を確保することができる,
② セキュリティに関連する情報を効率化した方法により迅速にコーディネーションをし,インシデント発生時の迅速な対応ができる,

ことを目指し,早急な標準化が求められている.

標準化団体の動きとしては特に IETF にて Incident Object Description and Exchange Format (IODEF) の標準化活動が行われている．IODEF は,インシデント関連情報の交換などに用いるフォーマットであり,インターネット標準である RFC 化を目指しており,インシデント報告フォーマットなどへの応用が期待されている.

3．提案方式

上記事項を踏まえ,広域におけるセキュリティインシデントを対象としたインシデント情報を送受信し保存できるようなシステムを設計した．各ネットワーク検知モジュールの情報・分析結果などのセキュリティ情報を統一のフォーマットに変換し,それを統合管理するものである．今回,統一フォーマットは IODEF にしたがって記録されるものとし,規定された情報交換方式に従って送受信するものとした．今回は特に受信部について設計／開発を行い,汎用的な通信インタフェースの実装を行った．通信経路におけるセキュリティ情報を取り扱いに考慮し以下の事項に注意することを念頭に置いた.

・情報が確実に伝わるようにする
・正確な情報を引き出す
・通信内容が漏洩する可能性への配慮を行う

3.1 設計

必要な機能としてセキュリティ情報送信機能,セキュリティ情報受信機能,セキュリティ情報管理機能を検討した．セキュリティ情報送信機能は IODEF フォーマットのセキュリティ情報を送信し,Web 画面ユーザーインターフェースを持つものとする.

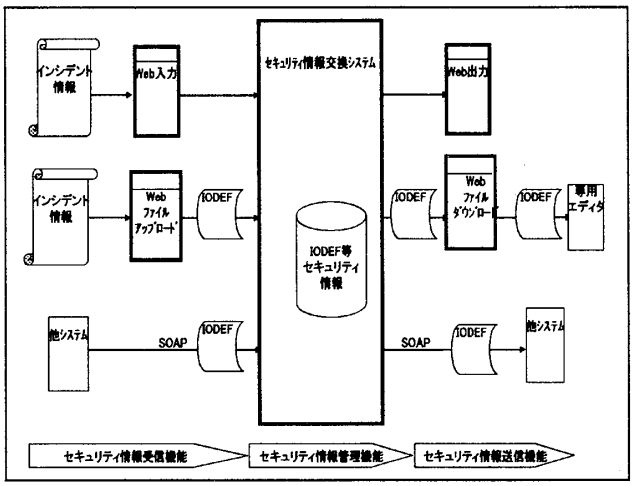

図1 セキュリティ情報交換モジュール概要図

†横河電機株式会社
CMK本部セキュリティプロジェクト

またIODEFファイルのダウンロードをHTTPとSOAPにて行うものとした．セキュリティ情報受信機能はIODEFフォーマットのセキュリティ情報を受信し，Web画面ユーザーインターフェースを持つものとした．セキュリティ情報管理機能はIODEFフォーマットのセキュリティ情報を格納するDBを持ち，DBに格納したIODEFフォーマットのセキュリティ情報をメンテナンスするためのユーザーインターフェースを持つものとする．また全文検索・ソーティング機能を持つものとした．

3.2 混在するスキーマへの対策

IODEFには複数のスキーマが混在しており，各システムにて取り扱うスキーマが異なるために情報交換が適切に行えなくなる可能性がある． 2005年6月現在公開されているIODEFのスキーマは0.23と0.30, 0.41の3つである．現在，他に行われているネットワーク監視情報交換システムにて扱っているスキーマのバージョンが0.23であることを参考にした．各機関が採用しているこれら各バージョンに対応することに加え，2005年夏以降に更新予定であるバージョン0.42に対応する必要があると考えた．

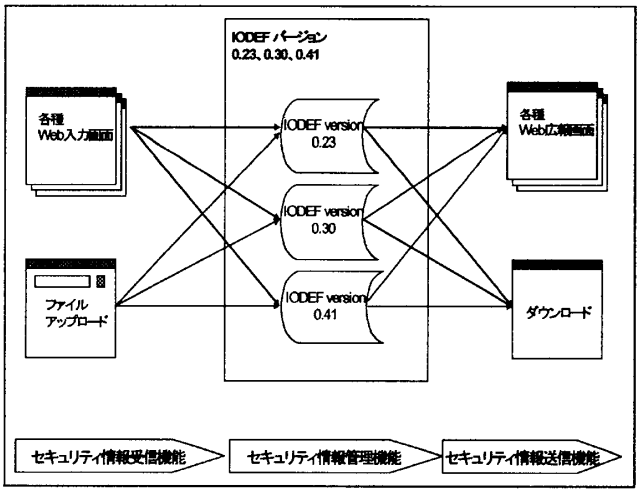

図2 スキーマの各バージョンの取り扱い

4．考察

上記設計したものを実際に開発して，セキュリティ情報の受信(登録)実験を行い動作の考察を行った．今回は，特に受信(登録)機能部分を開発した．システムの動作環境については，次のものを用いた．

- OS：Windows Server 2003 Standard Edition
- アプリケーション
  Internet Information Service
  (IIS) 6.0
- データベース
  SQL Server 2000 Standard Edition SP 3a
- ブラウザの環境
  Internet Explorer6.0 SP1

入力画面は，Web画面にて情報を入力させるため登録情報量が限られており，詳細な情報は伝えにくい．ただ初期情報であるため，最低限の情報内容が伝わればよいため，今回は最低限必要な情報をタイトルとレポート時刻とした．実際に作業をおこなうと，タイトルの表現次第で内容に誤解を与えてしまい，情報の再確認の作業が多くなることがわかった．初期情報であるので，タイトルについては入力者が明確に事実のみが伝わるように工夫をする必要がある．また，他の入力項目については，IODEFの項目数と比較してかなり少数ではあるが初期情報の報告という観点からは現状の項目数で対処できる．

次にデータの編集などのメンテナンスについて検討した結果，情報の誤りや追加情報などの編集を行う必要があり，その際には版管理が必要である．実際に運用すると送信機能作成の際には，IDとリビジョン番号が必要となった．またIODEFのスキーマは今後の動向によってはバージョンアップが考えられ適宜バージョンアップに対応する必要がある．今回はIODEFデータに対してスキーマによる検証を行うか否かを指定し，個別に検証の有無を指定することを可能とすることで別バージョンであっても対応を可能とした．

5．おわりに

本稿では，コンピュータセキュリティインシデントの情報交換を行なうものとして，IODEFを用いたセキュリティインシデント情報を受信して保存できるシステムを試作した．今後はこれら調査や考察を元に，インシデントに対してシステマチックに対処するためのプロトタイプシステムの設計を進める．また，情報内容の検討と設計を行い，送受信機能の作成を行う．さらにインシデントをオペレーションする手順を整理し，その手順に応じた処理を遂行しながら報告する際に必要となる報告の入力項目の検討を行う．

なお，本研究は情報通信研究機構(NICT)から「広域モニタリングシステムに関する基盤技術の研究開発」として受託し，実施中である．ここに記して謝辞を表する．

6．参考文献

[1] John D. Howard Thomas A. Longstaff, “A Common Language for Computer Security Incidents”, http://www.cert.org/research/taxonomy_988667.pdf

[2] CERT/CC, “CERT/CC Incident Reporting Form”, http://www.cert.org/reporting/incident_form.txt

[3] IETF INCH WG, ”Requirements for the Format for INcident information Exchange (FINE)”, http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-04.txt

[4] IETF Network Working Group , ”RFC 2350 Expectations for Computer Security Incident Response”, http://www.faqs.org/rfcs/rfc2350.html

[5] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski 他,”Handbook for Computer Security Incident Response Teams (CSIRTs)”, http://www.cert.org/archive/pdf/csirt-handbook.pdf