

広域インシデント情報共有および分析技術の開発

株式会社サイバー・ソリューションズ

2005年9月

1. はじめに

社会基盤としてのインターネット上に次々と起こる新しいセキュリティインシデントに対応するため、世界的な連携を強化する動きが活発化しており、国やISPを超えて連携(広域連携)できる新しいセキュリティシステムが必要とされている。

広域連携には、言語や特定のアプリケーションに依存しない標準化されたコミュニケーションの手段が不可欠である。そのため脆弱性情報の共有を目的として、世界各地のCERTが連携するための標準が提案され、IETFでは、そのためのメッセージ交換の標準(IODEF: Incident Object Description Exchange Format)を検討するINCH WG (Extended Incident Handling)が組織された。

本技術開発では、広範囲なインシデント情報の共有および分析技術に関する技術開発を目的とし、IODEFを活用した以下のようなシステムを開発する。

- ・ 広域不正アクセス追跡システム
- ・ 広域インシデント分析・警戒システム

上記によって、組織を跨いだインシデント情報の共有と、各地で試みられている定点観測システム[1]の連携にIODEFを活用し、より柔軟な連携を可能とする技術の確立を目指す。

2. 本開発の課題と期待される効果

本標準の早期普及と実践的なアプリケーションの構築を目指す。IODEF標準の活用と、その具体的な運用経験を示すことで以下のような効果が期待できる。

- ・ インシデント情報の自動で迅速な共有化
- ・ インシデントの広域追跡の実現
- ・ 広域インシデント情報のエンドユーザ活用

IODEF標準を用いてインシデント情報を広く配布、活用することで、インターネット全体の安全に大きく寄与することが期待できる。

3. 開発の概要

本開発は、基盤技術として、IODEF標準案をサポートするAPIを開発する。開発されたAPIを活用して、上記2種類の具体的なアプリケーションを開発する。

図1にIODEF標準が想定している基本モデルを示す[2]。

3.1. IODEF-API

最新のIODEF標準案(2005年8月現在)に基づいたAPIを開発した。図1のInterfaceの部分がAPIとして実装されており、CSIRTの部分で様々なアプリケーションを構築することができる。

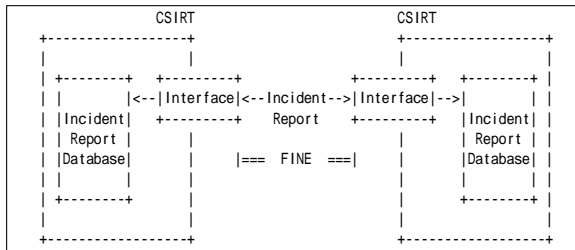


図 1 IODEF メッセージの概要

本実績は、IETF での議論にフィードバックするとともに、二つのシステムの基盤となっている。また、インシデントの届出フォームなどにも活用することができ、本開発で簡単な届出フォームも試作した（図 2）。

図 2 IODEF-API を活用したインシデント届出アプリケーション

本アプリケーションでは、エンドユーザからの一般的な届出を IODEF 標準に準拠した形で出力、送信することが可能であり、届出およびその処理プロセスの自動化に大きく貢献することが期待できる。

結果として、大規模なインシデント情報を早期に知ることが可能となり、早期の警戒、対応を

実現できる。

3.2. 広域不正アクセス追跡システム

送信元が詐称された不正アクセスの出所を特定するために、様々な技術が提案されており、そのうちのいくつかは実用的なレベルに達している。しかし全 Internet 規模で追跡を実行するためには、相互に運用できる標準化された技術が鍵となる。

本開発では、追跡システムの相互運用を目指して IETF で議論されている IODEF を拡張した IODEF-RID[3]を活用して、複数の独立した追跡システムを相互運用することを実現した。

本システムを基に標準化を推進することで、真の意味での広域追跡の第一歩とすることができる。

3.3. 広域インシデント分析・警戒システム

Internet で日々発生する不正アクセスは、DoS や Worm を初めとして多様化、広域化し、かつ非常に早く広まる傾向が強まっている。

一方で、企業や個人のセキュリティ管理者は、自サイトに訪れる様々なアクセスが妥当なものなのかどうかの判断をする必要があるが、Internet トラフィックは、多くの不正アクセスで汚染されており、それらの妥当性の評価は非常に困難である。

本分析システムは、インシデント情報を広域で共有するために議論されている標準化されたフォーマット IODEF で記述し、自動的に収集するとともに、その動向を分析するシステムである。応用として、現在、広く試みられている広域観測網を連携させることが可能となり世界的な不正アクセスの動向を効率よく知ることができる。それらを広く共有することで、

個々のサイト管理者がそれを参照して、判断の指標とすることも可能となる。

図 3 に、開発した広域インシデント分析システムの運用例を示す。様々な観測点で観測された情報は、標準化されたフォーマット (IODEF) で記述され転送される。本アプリケーションは収集された多地点の情報を統合することにより、ネットワーク全体で、広く観測されるインシデント (広域インシデント) を抽出することができる。

また、分析された結果を新たなインシデント情報として IODEF フォーマットで「Publish」することも可能であり、エンドユーザに分析された情報を提供することができる。

Detected Time	Reported Time	Incident Type	Source Address	Incident Name	Observation Point
2005/08/01 19:37:18	2005/09/27 13:15:36	Alert	60.181.2.211	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/01 18:47:03	2005/09/27 13:15:36	Alert	202.101.42.176	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/01 18:53:18	2005/09/27 13:15:36	Alert	217.205.84.130	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/03 15:11:32	2005/09/27 13:15:36	Alert	222.179.216.66	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/09 03:01:44	2005/09/27 13:15:36	Alert	91.153.0.102	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/13 16:30:29	2005/09/27 13:15:36	Alert	222.136.87.240	ICMP PING NMAP	csirt.cysoils.com-20
2005/08/22 00:41:58	2005/09/27 13:15:36	Alert	93.237.115.24	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/21 02:08:14	2005/09/27 13:15:36	Alert	222.174.115.18	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/11 12:38:07	2005/09/27 13:15:36	Alert	203.121.88.9	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/13 14:25:39	2005/09/27 13:15:36	Alert	222.178.152.96	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/18 00:52:51	2005/09/27 13:15:36	Alert	221.236.9.54	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/01 21:47:24	2005/09/27 13:15:36	Alert	220.176.14.200	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/07 08:01:31	2005/09/27 13:15:36	Alert	202.99.177.209	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/05 19:58:05	2005/09/27 13:15:36	Alert	202.180.140.8	MS-SQL Worm propa.	csirt.cysoils.com-20
2005/08/07 13:38:09	2005/09/27 13:15:36	Alert	221.236.9.54	MS-SQL Worm propa.	csirt.cysoils.com-20

図 3 広域インシデント分析

3.4. 広域インシデント情報の可視化

図 4 に本システムで実現した可視化例を示す。本開発ではインターネット規模の広域に影響を及ぼすインシデントを対象としている。本可視化システムでは、インシデントの発生日点をネットワーク地図上に示すことで、その広がり、影響範囲、拡散傾向を分析することができる。

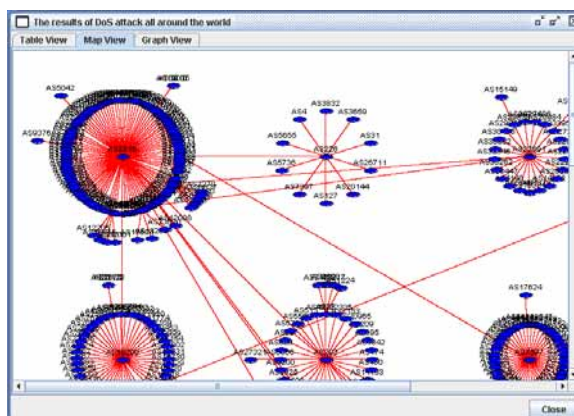


図 4 広域インシデントの地図による可視化

4. まとめ

本開発によって、IODEF 標準を活用するための基盤技術を確立することができた。また、具体的な応用例となるアプリケーションを開発し、その有用性を示すことができた。

今後は、本標準に基づく情報収集を推進するとともに、本技術および、分析結果のエンドユーザによる活用の可能性を検討していくことで、インターネット全体の安全と安心に寄与することが期待される。

5. 参考文献

- 1 独立行政法人 情報処理推進機構, “「インターネット定点観測システム」について”, <http://www.ipa.go.jp/about/press/20040511.html>, 2004 年 5 月 11 日
- 2 Yuri Demchenko, Hiroyuki Ohno, Roman Danyliw, Glenn M Keeni, “Requirements for the Format for Incident information Exchange (FINE)”, Internet-Draft, Work in progress, September 7, 2005
- 3 Kathleen M. Moriarty, “Incident Handling: Real-time Inter-network Defense”, Internet-Draft, Work in progress, September 19, 2005