社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

ぼくの地球を守って

サイバー戦争の悲惨さを伝えるセキュリティ可視化技術の研究

なまやつはし† 　ういろう†

† Project PACKTER　http://www.packter.jp, Japan
E-mail: †{namaya2hashi,uirou}@packter.jp

あらまし　本論文は新しいサイバーセキュリティ可視化ソフト PACKTEARTH を提案する．他の可視化ソフトとは異なり，PACKTEARTH はサイバー戦争の悲惨さを訴えるための目的において開発されたソフトウェアである．これまで人類は多くの戦争を経験してきたが，二度と戦争を繰り返さないため戦争の悲惨さを後世に伝えている．本研究はこの概念を拡張し，サイバー戦争を繰り返さないためにも同様の試みが必要ではないかと考える．この発想に基づき，PACKTEARTH は大陸弾道ミサイル及び着弾による爆発によって攻撃を表現する．本論文は，悲惨さを伝える本提案が有効であるかどうかを着目するため．被験者を集めた実験を通じて検証を行う．
キーワード　セキュリティ 可視化 サイバー戦争

Save Our Planet

Security visualization for conveying the horrors of cyber war

Namaya2hashi† and Uirou†

† Project PACKTER　http://www.packter.jp, Japan
E-mail: †{namaya2hashi,uirou}@packter.jp

Abstract　This paper proposes a novel security visualization software, named PACKTEARTH. Aside from existing visualization tools, PACKTEARTH is designed to convery the horrors of cyber war. Humanity has gone through many wars, and in order to prevent any more war, it is important that the converying to everyone the horros of way. We extend this concept for cyber war, that is, the dissermination of the horror, severity, and/or cruelty of cyber war is also important to prevent cyber war. PACKTEARTH represents each attack with intercontinental ballistic missile and bombing. Based on the concept, this paper conducts a participant-based experiment and examine the effectiveness of our proposal to convey the horror.
Key words　Security, Visuzaliation, Cyber War

1. はじめに

近年，サイバー攻撃が激化しており，攻撃の対策は急務である．サイバー攻撃はコンピュータネットワーク，コンピュータネットワーク接続するシステム，プロトコル及び様々なユーザや管理者などのステークホルダーなどによって構成されるサイバー社会を対象に行われる攻撃である．サイバー社会がいっそうの発展を遂げるためには，サイバー社会を攻撃から守る技術が開発されている．しかし，防御する技術をかいくぐろうとするため，サイバー攻撃技術も日々複雑化しており，サイバー攻撃への対策は未だ十分ではない．

サイバー攻撃の可視化は，複雑化したサイバー攻撃の対策を行うために重要であると考えられている．可視化とは本来，人間が直接見ることができない事象の関係性を見える形状に変換することであり，人間が元来保有している認知能力を攻撃の解析に役立てようという技術である．可視化により，サイバー攻撃の存在に気づくだけでなく，サイバー攻撃の対象や影響もわかり，どのような対策が有効かを決定しやすくなる．可視化技術を複雑化したサイバー攻撃対策に役立てようという研究は NICTER [1] などが挙げられる．

さて，サイバー攻撃はサイバー戦争とも言われることがある．日本は憲法第 9 条において戦争を放棄している通り，日本人は国際平和を誠実に希求する民族である．しかし，サイバー戦争についてはどうか．サイバー攻撃，サイバー戦争の可視化は何

をもたらしたのか．見た目の美しさだけにとらわれ，サイバー戦争の悲惨さ，酷さを伝える努力は怠ってはいないだろうか．サイバー戦争を二度と繰り返さないようにする平和の心は，サイバーセキュリティの研究者の一人ひとりが持つべきであるというのが著者の信念である．それはサイバーセキュリティの可視化という問題ついても同様である．

そこで，可視化技術を通して，サイバー戦争の悲惨さを可視化するシステムを提案する．サイバー戦争の際に使われる通信はいわば兵器であり，それは殺傷力の高い悲惨な武器として描かれるべきである．すなわち，パケットはミサイルであり，着弾点から爆散したものが描かれるべきはかなろうか．本論文では可視化された画面を通じてこそ，サイバー戦争の悲惨さを人類に訴求できるという仮説をおく．なお，サイバー攻撃は一般に米国と中国の間で行われるとされるが，ロシアやヨーロッパ，そして日本もしばしば関係している．正確には日本にあるサーバが狙われたり，日本にあるボットネットが攻撃に利用されている．本論文では，この状態を「日本がサイバー戦争に参戦している」と定義することにする．

本論文で開発する PACKTEARTH は，地球儀状の平面に各国から各国へのサイバー攻撃が大陸弾道ミサイルとして表示され，戦争の悲惨さを伝えるシステムである．また，可視化技術は視覚障害者には扱いにくい技術であるが，この問題を解決するため爆発音などの音響にて本研究の目指すサイバー戦争の悲惨さを伝えることができるよう設定した．このソフトウェアを学生 X 名のアンケート調査により評価を行い，他のソフトウェアとくらべてサイバー戦争の悲惨さをより伝えられているかどうかを示すことによって評価実験を行った．統計的仮説検定の結果，PACKTEARTH はサイバー戦争の悲惨さをより表現できるという事象が確認された．

本論文の構成を以下に示す． 2. 節において先行研究と問題点を分析し， 3. 節において PACKTEARTH の設計を， 4. 節において実装を示す． 5. 節において被験者実験の結果を述べ，最後にまとめと今後の課題を 6. 節に示す．

2. 先 行 研 究

本節では本研究に関連する研究を紹介する．まず，サイバー攻撃の可視化についての現状を 2.1 節において，次に戦争の悲惨さを訴える取り組みを 2.2 節に示す．

2.1 サイバー攻撃の可視化の研究

サイバー攻撃の可視化については，2005 年ごろの奈良先端科学技術大学院大学のインターネット工学講座 (注1) において盛んに行われており，その成果が衛藤将史，鈴木未央を通じて独立行政法人情報通信研究機構 (注2) に伝わったとされる一方で，著者らのグループもこの研究を継承している．同じ研究室では，櫨山寛章，松本義秀のサイバー攻撃の可視化ソフト QT Traceback Viewer [2] が開発されている．国内最大級のネットワーク展示会である Interop Tokyo 2010 では，NICT に在籍した著者らが PACKTER [3] を，衛藤らの研究グループが NICTER を，奈良先端大の協力という形で櫨山らの研究グループが QT Traceback Viewer を展示するという一幕もあった．

NICTER [1] は NICT によって開発された，サイバー攻撃やマルウェアの挙動をダークネットにおいて観測し，その内容を可視化するソフトウェアである．ダークネットとは特定のホストコンピュータが割り当てられていない IP アドレス空間であり，そのアドレスへの通信は正常な通信ではなく，DoS やスキャン，バックスキャッタなどのサイバー攻撃の可能性が高い．NICTER の可視化は，送信元と送信先のアドレスに基づいて三次元空間に浮かぶ立方体の中にアニメーション表示する Cube，世界地図や地球儀上に表示する Atlas がある．

QT Traceback Viewer は，IP トレースバック技術の可視化目的に開発されたソフトウェアである．近年の DoS では，送信元 IP アドレスを偽装したパケットが利用されており，このような攻撃を緩和するため自律分散システム（Autonomous System, AS) をまたがったパケット追跡システム InterTrack [4] が開発されている．このシステムのデモには，当然 AS 間の連携構成を表現する仕組みが必要となり，櫨山らはインターネットを模倣するテスト環境を研究し [5]，これを可視化するソフトウェア QT Traceback Viewer を開発した．QT Traceback Viewer は，二次元平面に表示する球状の物体によって AS を，その間の線によって隣接構造を表現する．この隣接構造の上に大きな矢印を用い，DoS 攻撃の追跡の様子を描画する．

NICTER の問題はオープンソース・ソフトウェアではないため改良ができないことであり，NICTER と QT Traceback Viewer に共通する問題は，どちらも美しさ，直感的なわかりやすさ等を主眼としたソフトウェアにとどまっている点である．これらの可視化画面を見た人間が抱く感情はポジティブな内容が多く，サイバー戦争の悲惨さを訴える上では逆効果となる可能性がある．

我々は先行研究を反面教師とし，可視化画面を見た人間にポジティブとネガティブな感情の両方を抱かせる工夫を検討した．PACKTER [3] は，名前が「パクッター」と発音される通り，まるでアイデアを盗用したのではないかと錯覚させる．しかし，直接的に嫌悪感を抱かれることのないように，あるいは初見者に興味を持ってもらえるように，ネガティブな感情だけではなくポジティブな感情も抱いてもらえるように，イラストは「あの蒼い海より」 [6] の作画担当をされたユイザキカズヤ氏，サウンドは「ラッキードッグ 1」 [7] の作曲担当をされた SENTIVE 氏に依頼し，18 歳以上の男女の両方に訴求できるよう考慮した．

しかし，これらの研究全ての問題点として，これまでサイバー戦争の悲惨さを訴えるような取り組みは行われていないことが挙げられ，本研究はこの問題の解決を目指す．

2.2 戦争の悲惨さを訴える活動

1. 節に述べた通り，日本は憲法第 9 条において戦争を放棄し，日本人は国際平和を誠実に希求する上で，二度と戦争を繰り返さないために戦争の悲惨さを訴える膨大な活動が行われて

(注1)：インターネット工学講座, http://iplab.naist.jp

(注2)：National Institute of Information and Communications Technology (NICT), http://www.nict.go.jp

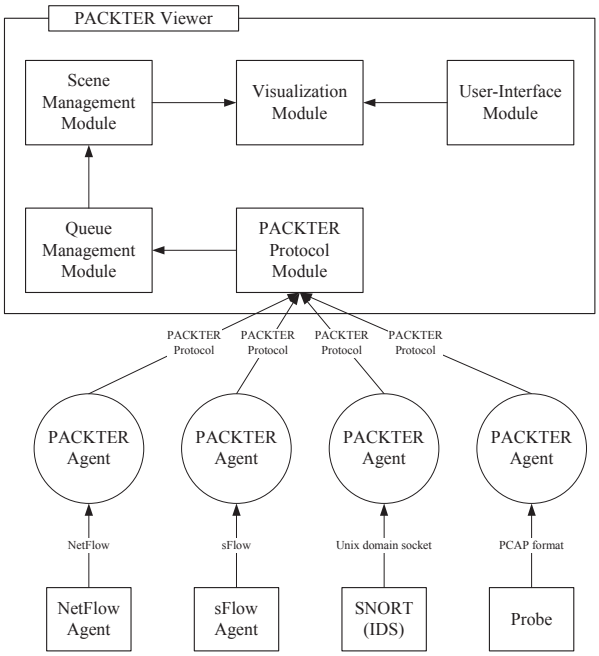

図 1　PACKTER のアーキテクチャ

おり枚挙に暇がない．戦争の悲惨さを語る上では，例えば家族や友人の生命が失われること，戦中・戦後の貧困生活といったミクロな視点のみならず，原子爆弾が日本に着弾するといったマクロな視点でも語られている．

サイバー戦争のおいて，生命が失われる可能性は現実の戦争に比べて少ないといえる．医療機関の電子カルテなどの情報の改ざんや紛失，あるいは利用可能性が損なわれるなどの攻撃によって命が損なわれるケースは想定されるものの，戦争への徴兵や市街地への攻撃と比べると生命への殺傷性は低いといえる．また，サイバー戦争に伴う貧困も，例えば昼夜問わず行われる攻撃に対応するため，オペレータが昼夜問わず最大の注意を持って対応するなどの予期せぬ労務が発生することに伴う貧困などが想定されるものの，やはり戦争への徴収や生活インフラに対する攻撃と比べると影響は低い．

本論文では，ミクロな視点から戦争の悲惨さ訴えることは重要ではあるとしながらも，それは次の研究目的と位置づける．そして，マクロな視点から戦争の悲惨さを訴えることを目的とする．このため，国土への爆弾の着弾を通じ，サイバー戦争を訴える可視化を実現する．

3. PACKTEARTH の設計

PACKTEARTH の設計にあたり，我々が開発してきた PACKTER [3, 8] のアーキテクチャを参照することとした．PACKTER はエージェントとビューアの 2 つのプログラムによって構成される．エージェントはパケット単位の情報収集を行い，その内容をビューアに送信するプログラムであり，ビューアはこの内容に基づた描画を行うプログラムである．

PACKTER のアーキテクチャを図 1 に示す．PACKTER エージェントは (1) ネットワーク情報収集を通じたデータ収集，(2) トラフィックを保存したファイルを通じたデータ収集，(3) トラフィックサンプリングプロトコルを通じたデータ収集，そして (4) UNIX ドメインソケットを通じたデータ収集である．(1) 及び (2) の機能は一般的なパケット処理ライブラリである PCAP [9] を用いて実装する．(3) の機能は sFLow 4.0 [10] や NetFlow 9.0 [11] でいうところのフローコレクタ機能の実装により実現する．(4) の機能は他のプログラムとのデータ通信のために用いられる．例えば IDS として著名な SNORT [12] はサイバー攻撃を検知する機能を備えており，検知結果を UNIX ドメインソケットを用いて出力する機能を備えている．エージェントはこの内容を読み取ることで，サイバー攻撃の情報を得られる．

表 1　PACKTEARTH のプロトコルフォーマット

```
PACKTEARTH\r\n
SRC LAT,SRC LON,DST LAT,DST LON,FLAG,DESCRIPTION
```

表 2　ミサイルの設定

#	ミサイルの種類	ネットワーク層	トランスポート層	フラグ
1	AM39	IPv4	TCP	ACK
2	AS-20	IPv4	TCP	SYN
3	AS-30	IPv4	TCP	FIN or RST
4	ASM-1	IPv4	UDP	
5	Bullpup-A	IPv4	ICMP	
6	Bullpub-B	IPv6	TCP	ACK
7	C-801	IPv6	TCP	SYN
8	Gabriel	IPv6	TCP	FIN or RST
9		IPv6	UDP	
10		IPv6	ICMP	

PACKTER ビューアは 5 つのモジュールによって構成されている．まず，PACKTER Protocol モジュールは UDP ポート番号 11300 においてサーバを起動し，エージェントの送信するパケット内容を読み取り，制御キューに追加する．(注3)Queue Management モジュールは，キューに追加された情報のタイムスタンプを読み取り，適切な時間に描画されるよう管理を行う．Scene Management モジュールはタイムスタンプを元に画面描画を行う機能を提供し，Visualization Module がパケットを送信元から送信先あてに描画する．残りのモジュールはキーボードやマウスによる操作を受け付けるモジュールである．

PACKTEARTH エージェントは PACKTER プロトコルを表 1 のように拡張する．`PACKTEARTH` というプロトコルヘッダに続き，カンマによって区切られた 6 種類の情報が送信されている．この情報は送信元の緯度，送信元の軽度，送信先の緯度，送信先の経度及びフラグとパケットの概要である．フラグはミサイルの種類を表現する際に用いられる．

4. PACKTEARTH の実装

図 2 に PACKTEARTH における可視化画面，表 2 にミサイルの意味を示す．AM39 とはロシア製のミクーリン AM-39，AS-20 及び AS-30 はフランス製のミサイルである．ASM-1 は日本製の 80 式空対艦誘導弾，Bullpup-A 及び B はアメリカ製の AGM12 ミサイルである．C-801 は中国製のミサイル，Gabriel3 はイスラエル製のミサイルである．(あとで確認する)

弾道計算は Shoemake [13] の提案する Slerp アルゴリズムを

(注3)：プロトコルの詳細については文献 [8] を参照されたい．

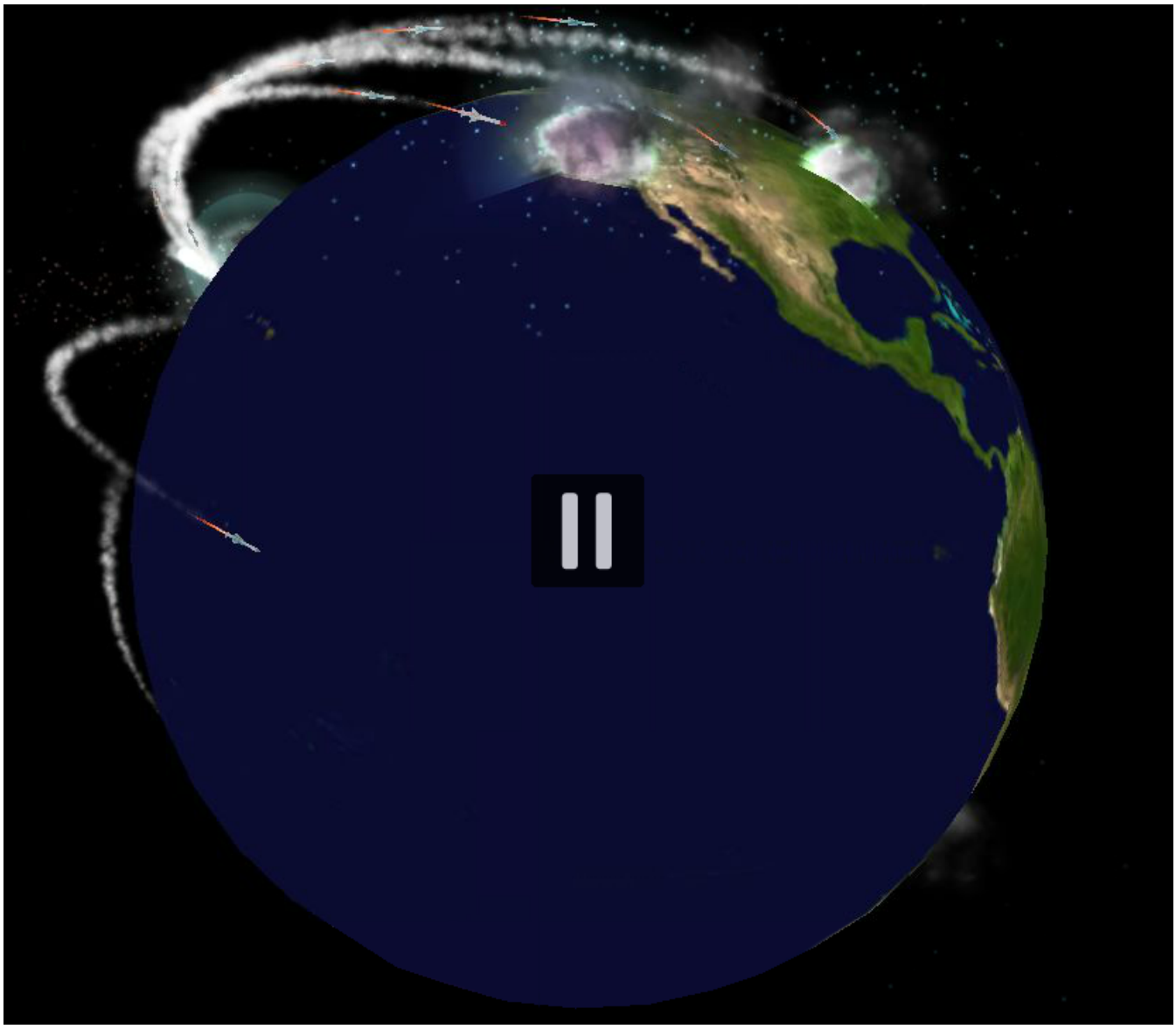

図 2　PACKTEARTH における可視化画面

採用する．3D 画面における座標系となる値（x, y, z 座標）という 3D 空間上の軸と，その軸を中心とした回転によって構成される 4 次元ベクトルは，クォータニオンと呼称される．Slerp アルゴリズムはクォータニオン同士の球面線形補間を行うアルゴリズムであり，式 1 のように一般化されている．数式において p_0, p_1 は弧の始点と終点であり，Ω は回転をラジアンで表現した値，t は $0 \leqq t \leqq 1$ となるパラメータを示す．

$$\mathrm{Slerp}(p_0, p_1; t) = \frac{\sin[(1-t)\Omega]}{\sin\Omega} p_0 + \frac{\sin[t\Omega]}{\sin\Omega} p_1 \qquad (1)$$

また，弾道計算においては，最短距離をとるようなアルゴリズム 1 を実装した．ABS は絶対値を求める関数，$from$ は送信元，to は送信先の緯度・経度などの座標である．北緯と南緯は（どうしているんだっけ）また，正の値，負の値によって移動する方向が異なる．

Algorithm 1 最短距離計算のアルゴリズム

```
if (ABS(from) − ABS(to)) < 180 then
    ret = from − to
else
    if ABS((ABS(from)−ABS(to))+360) > ABS((ABS(from)−
    ABS(to))) − 360)) then
        ret = from − to − 360
    else
        ret = from − 30 + 360
    end if
end if
```

5. 被験者実験による評価

6. お わ り に

文　　献

[1] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J.

Nakazato, K. Ohtaka, and K. Nakao, “nicter: An Incident Analysis System toward Binding Network Monitoring with Malware Analysis,” Proceedings of WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp.58–66, Apr. 2008.

[2] H. Hazeyama, Y. Matsumoto, and Y. Kadobayashi, “QT Traceback Viewer,” Available at: `http://intertrack.naist.jp`.

[3] D. Miyamoto and T. Iimura, “PACKTER: implementation of internet traffic visualizer and extension for network forensics,” Journal of Computing, vol.96, pp.79–80, Jan. 2014.

[4] H. Hazeyama, Y. Kadobayashi, D. Miyamoto, and M. Oe, “An Autonomous Architecture for Inter-Domain Traceback across the Borders of Network Operation,” Proceedings of the 11th IEEE Symposium on Computers and Communications, pp.●●–●●, Jun. 2006.

[5] H. Hazeyama, M. Suzuki, S. Miwa, D. Miyamoto, and Y. Kadobayashi, “Outfitting an Inter-AS Topology to A Network Emulation TestBed for Realistic Performance Tests of DDoS Countermeasures,” Proceedings of Workshop on Cyber Security and Test, pp.●●–●●, Jul. 2008.

[6] L. Soft, “あの蒼い海より,” Available at: `http://www.lilacsoft.jp`.

[7] Tennenouji, “ラッキードッグ 1,” Available at: `http://www.tennenouji.net`.

[8] D. Miyamoto and T. Iimura, “Design and Implementation of PACKTER,” Technical report, Project PACKTER, Dec. 2014.

[9] The Internet Society, “PCAP Next Generation Dump File Format,” Available at: `http://www.winpcap.org/ntar/draft/PCAP-DumpFileFormat.html`.

[10] P. Phaal, S. Panchen, and N. McKee, “InMon Corporation’s sFlow: A Method for Monitoring Traffic in Switched and Routed Networks,” RFC 3176, IETF, Sep. 2001.

[11] B. Claise, “Cisco Systems NetFlow Services Export Version 9,” RFC 3954, IETF, Oct. 2004.

[12] Snort, “The Open Source Network Intrusion Detection System,” Available at: `http://www.snort.org/`.

[13] K. Shoemake, “Animating Rotation with Quaternion Curves,” Proceedings of the 12th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH), pp.245–254, July 1985.