Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

インターネット空間の汚れ具合を観察するインタフェースの提案

斉藤　典明

サイバー攻撃に代表されるようにインターネット空間には様々な脅威がある。しかしながら、多くの利用者はどのくらいインターネット空間に危険性があるのかを把握するすべがない。そこで、現在まだ主流である IPv4 アドレスの 32bit 全領域に対する時系列データをプロットできるインターネット空間を Web ブラウザ上に構築し、アクセスログや危険なサイトのアドレス情報をプロットすることにより自分自身の普段の利用行動においてどのくらい危険なサイトに近づいているかを観察できるインタフェースを開発したので報告する。

A Interface for Observation of the Internet Space

SAITO Noriaki†

There are a lot of threats in the Internet, for example, cyber attack. However, we have few ways of perceiving danger at the Internet space. To solve such problem, an interface was developed which enables to observe risk in the Internet space. In the interface, the Internet space is expressed by the full scale IPv4 address and a time scale, and access log data and dirty site address are plotted on the space. In this paper, the structure of the interface is shown and effect of using the interface is considered.

1. はじめに

ここ 1～2 年の間に急速にサイバー攻撃に対する脅威が増加している。インターネット利用における脅威は従来のような個人レベルの「いたずら」や「能力の誇示」が目的の攻撃から、組織ぐるみによる「金銭目的」や「組織活動の妨害」が目的の攻撃に変化してきている[1]。

例えば、一般のインターネット利用においては通常の Web サーバが改ざんされ、攻撃コードが埋め込まれ知らない間にマルウェアに感染してしまうドライブバイダウンロード攻撃が増加している。また、企業や政府系機関などでは標的型攻撃と呼ばれる攻撃によりアンチウィルスソフトなどをすり抜けて気が付かないうちにマルウェアに感染してしまう脅威が増加している。

このような脅威の増加に対して、ネットワーク装置および運用技術として次世代ファイアウォールや標的型対策システムなどの導入により、マルウェアの感染防止や感染後の早期発見を行いネットワークを安全に利用するための環境が整いつつある。一方で、一ユーザとしては、感染後の判定はわかりつつあるものの普段の利用においてどの程度危険なのか、どのようにふるまえば危険を回避できるのか、について把握する方法が少ない。例えば、インターネット上の個々のアドレスに対して接続先が安全か危険かを判断するすべがある。しかしながら、攻撃者は常にアドレスを変化させるなど追跡を困難にしているため個々のアドレスの判定が正しいとは限らない。結局、複数の判定結果を参考に接続先アドレスの危険性を判断することになる。

このような場合、もし自分自身の接続先のデータについて様々な観点から十分に観察できるようになれば観察結果に基づいて利用行動を判断できると考えられる。現在はまだ IPv4 アドレスが主流であり、IPv4 であればアドレス帯は 32bit 長で高々42 億個、グローバルアドレスとして利用するのは 37 億個程度である。そこで、この 42 億個の IP アドレスに対して、ユーザ自身が分かっている範囲の様々な情報を蓄積してゆき、普段の利用行動と対比することにより、不審なサイトには近づかないような行動をとることができるようになると考えられる。

このような狙いのもと、今回、通信ログを IP アドレスと時系列でプロットできるインターネット空間を Web ブラウザ上に構築し、アクセスログや不審なサイトのアドレス情報をプロットすることによりインターネット空間の汚れ具合を観察し、利用行動の判断の参考にできるインタフェースを開発したので報告する。

2. インターネット空間の可視化

インターネット空間上に危険なサイトがどのくらいあり、どのくらいの頻度でどこからどこに攻撃をしているのかは完全には把握できていないが、様々な観測方法で攻撃情報の増加は伝えられている。例えば、nicter[2]ではダークネットで観測された攻撃情報を 3D 表示で可視化している。あるいはハニーポットで観測された攻撃データの IPv4 アドレスについて２次元のヒルベルト曲線で表現した空間にマッピングすることによりヒートマップとして可視化する手法などがある [3][4]。

これらの情報によればインターネット上には非常に多くの攻撃があることが実感できる。しかしながら、これらのデータから、ネットワークのフィルタや感染端末の特定など具体的な行動には移すには情報が足りない。特に、攻

† NTT　セキュアプラットフォーム研究所
NTT Secure Platform Lab.

Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

撃手法も巧妙になっているため一ユーザにとっては、攻撃されていても自覚することが難しい。また、ネットワーク管理の現場においては、IDS などで検出された不審なアクセス先、通信ログ中の不審なアクセス先は大量にあり、これらの中から選別しネットワークのフィルタ設定、ユーザ端末の特定・マルウェアの駆除、ユーザへの注意喚起などのアクションにつなげてゆくには、より詳細化した情報が必要になる。

そこで、検知された不審な通信先アドレスの安全性や危険性を具体的に知りたい場合、一つの方法として危険な通信先のアドレスを集めた情報リスト[5]の活用がある。検出された通信先のアドレスがこのような情報リストに掲載されていれば危険な通信先と判断ができる。あるいは、情報リストそのものはわからなくても、装置内に組み込まれた様々なカテゴリの危険な通信先の情報リストに基づいて遮断またはアラート（警告）を実施し、遮断またはアラートをどのカテゴリで実施したかを知る仕組み[6]の活用がある。

しかしながら、これらの方法では、結果が安全・危険の２値的なものになるのと、そもそもインターネット上のすべてのサイトを評価した上で判別しているわけではないため本来は多数の未判定や誤検知・検知漏れが発生する。特に、大規模に集めた危険なサイトの情報リストであっても複数のセンサで検知したアドレスは容易にマッチしないことも報告されている[7][8]。このことからインターネット上のアドレスに対して単独情報リストで判断するには限界がある。

これは、アドレス空間に対して不審な利用者が少ないという原因も考えられるが、サイバー攻撃が増え深刻になっている現在では、それよりも攻撃者が tor などの接続元のアドレスをかく乱する仕組みの利用、踏み台サイト、bot ネット等により一般利用者に紛れ追跡を逃れる方法、観測者に応じて振る舞いを変える仕組みなどにより単独での網羅的な情報リストの作成が難しくなっていると考えるのが自然である。さらに、ネットワークの仕組みとして、特に、IPv4 アドレスは枯渇しており、DHCP や NAT の利用により、アドレスの使い回しなどにより IP アドレスで端末を特定できない。また、ホスティングにより同じサーバ上で様々なユーザが共同利用しているため、同じ IP アドレスに安全なユーザと危険なユーザが同居していることもありうる。これらのことから、通信先アドレスを見た時、そのサイトが安全なのか危険なのかを単純に判別することができない。検出された不審な通信先の判別においては、様々な組織が提供する危険なサイト [9]-[16]の検索結果や whois などによりアドレスの登録情報を参考にし、ユーザ自身が判断することになる。ただし、不審な通信先が攻撃サイトであるとわかった時にはすでに攻撃を受けていることになる。

一方、インターネット空間上には、危険なサイトが多いアドレス帯があるなど偏りがあり、その領域も変化している。このような、インターネット空間の特性を知った上で普段の利用行動において危険なサイトへ近づかないような回避行動をすることができれば、危険なサイトへ近づくリスクを減らすことができると考えられる。そのためには、情報リストにおいて安全、危険という２者択一ではなく、危険な領域に近いのかそうでないのかなど、危険な度合までを知ることができると良い。これを実現するためには、特にこれまでの情報リストは危険なサイトの情報収集が中心であったが、危険なサイトの情報だけでは判断できないことが多く、危険なサイト、安全なサイト、所有者などわかっている範囲の様々な情報を IP アドレス空間にマッピングし、インターネット空間の全体状況を把握した上で判断できる必要がある。

そこで、普段のアクセスログを IP アドレス空間上にマッピングし観測することにより現在の利用形態の危険性を自分自身で判断できるインタフェースを提案する。

3. 想定利用モデル

自ネットワークの通信ログを観察することを目的とし、想定される利用者は、エンドユーザとして自分自身のアクセス先の検査を行う立場の他、企業などのネットワーク管理者としてファイアウォールやサーバのアドレスリストを管理するオペレータを考える(図 1)。両者の立場におけるニーズを整理すると表１のようになる。

（１）エンドユーザの観点：多くのエンドユーザは所属するネットワークが提供するセキュリティサービスや市販のアンチウィルスソフトにより自分の端末の安全性を確認することができる。しかしながら、普段の利用においてアンチウィルスが反応するのは攻撃を受けてしまった時であり、危険なサイトに近づいたかどうかまでは判別しない。つまり、事前に危険回避行動をとるための仕組みではなく、もし事前に把握できれば有用になると思われる。

（２）ネットワーク管理者の観点：ネットワーク管理者の立場では、ネットワークに入ってくるトラヒックとネットワークから出てゆくトラヒックを監視している。ネットワークに入ってくるトラヒック監視は入口対策と呼ばれ、ネットワークの接続ポイント、公開 Web サーバやメールサーバが DOS 攻撃や不正アクセスの対象になっていないかを確認し防御を行う。IDS 等での検知や市販のブラックリストに基づきファイアウォールや Web Proxy で遮断するなどの対策を行う。

しかしながら最近は、攻撃が巧妙になり従来のような入口対策だけではネットワーク内を守れなくなっている。そこで、出口対策と呼ばれる攻撃を受けたあとの被害を最小限に抑える対策方針を行う。そこでは、ネットワーク内の端末のアクセス先を監視し、その中にマルウェアに感染した端末がアクセスする先があった場合、感染端末を早急に特定し駆除を行うなどの対処を行うことが必要になってい

Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

る。

これらの場合、市販セキュリティ製品などに含まれる既存の情報リストでは誤検知が多く対応が難しい。そのため普段の自ネットワークの利用状況と見比べて不審なアクセスなのかそうでないかを判断することになる。このとき、危険なサイトの情報リストだけでなく、普段の利用状況とあわせて判断できれば有用になると思われる。

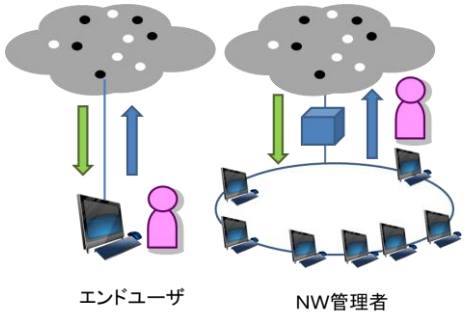


図 1.利用想定モデル

表 1. 想定利用シーンにおける要件

立場	外部からのアクセス	外部へのアクセス
エンドユーザ	・自分の PC／サーバが外部から侵入を受けていないかどうかを確認したい **・自分が攻撃を受ける可能性があるか知りたい**	・自分が感染していないか確認したい **・危険なサイトに接続しそうか知りたい**
NW 管理者	・自ネットワークが外部から攻撃を受けていないかを確認したい ・検知したアラートログを確認したい ・遮断リストをチューニングしたい **・普段の利用状況と見比べて判断したい**	・組織内ネットワークから危険なサイトへ接続しているかどうかを確認したい（ユーザへの注意喚起） ・感染端末の存在を知りたい ・検知したアラートログを確認したい ・遮断リストをチューニングしたい **・普段の利用状況と見比べて判断したい**

4. 提案インタフェース

想定利用モデルにおいて、市販のセキュリティ製品による判定では自のネットワークにおける判定ではないために判断がつかないという問題を解決するために、自ネットワークのログをインターネット空間全体にマッピングし自ネットワークの安全性・危険性を直観的に把握できるインタフェースを提案する。

この観測用インタフェースを提案にあたって、インターネット空間として依然として主流である IPv4 のアドレス空間を扱うこととする。IPv4 アドレスは IPv6 に比べアドレス空間が小さいが、PC の画面で表示するにはアドレス空間は広大すぎ、IP アドレス空間をそのまま表示したのでは全体像が把握できない。そこで、インターネット空間を鳥瞰でき、必要に応じて詳細化と様々な情報とのマッチングを行う仕組みを Web ブラウザ上のインタフェースを HTML5 の canvas オブジェクトで実装した。このインタフェースの狙いは３つあり（１）アドレス空間と時系列の表示、（２）鳥瞰と詳細化（３）データの比較である。

（１） アドレス空間と時系列の表示：

アドレス空間と時系列の表示をするために、提案インタフェーの基本パーツとして図2のように縦軸にIPアドレス空間、横軸に時系列をとる。

Web ブラウザ上で IPv4 アドレス空間すべてを一次元表示できない。また IPv4 アドレスの特性上 8bit 単位で領域を指定するのが望ましい。8bit は 256 ドットになるが IPv4 アドレスを 8bit で集約してしまうのは粗すぎる、24bit である 167 万ドットでは広すぎる。そこで縦軸のアドレス空間として 16bit である 6 万 5 千ドットで表示することとした。

ログデータを蓄積し、じっくり分析することを目標とし、リアルタイム性のインタフェースではないため、横軸の時系列データは 1 ドットを 1 日単位で表示することとした。

（２） 鳥瞰と詳細化：

16bit の軸では、IPv4 のすべてのアドレス空間を表現することができない。そこで、この 16bit のアドレス空間に対して、インタラクティブな操作により IPv4 アドレス空間を鳥瞰と詳細化することにより全体像を把握する仕組みとした。

具体的には、IPv4 アドレスの上位 16bit で集約した空間、第一オクテッドで指定される空間を第二オクテッドと第三オクテッドの 16bit で拡大した中程度に粗い空間、第一オクテッドから第二オクテッドまでで指定される空間を第三オクテッドと第四オクテッドの 16bit で拡大して詳細化した空間の３つを用意した。これらの空間を行き来し、アドレス空間内を鳥瞰画面から必要に応じて詳細化してゆくことにより観察を行う(図 3)。

（３） データの比較：

次に、基本パーツと基本パーツを組み合わせることにより鳥瞰と詳細化のできるアドレス空間に、観察したデータのプロットを行う。扱うデータとして、通信ログのような発生事象のデータと、悪性サイト情報のような半ば定性的なデータの２種類とする。

発生事象のデータは日付と IP アドレスにより指定され

Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

る位置に点で表示する。点については発生事象の種類に応じて色分けや、発生事象の多さに応じた大きさで表現する(図 4)。

情報リストのような定性的な情報は、時間的な要素は無視し、時間軸へのマッピングは行わず、IP アドレス軸のみにマッピングする。情報リストは考え方によっては発行日などにより日付を指定することは可能であるが、発行日が情報の特性を表しているわけではないため時間的な要素は無視することとした。そのため IP アドレス軸のみのマッピングのため、時間軸は全領域に渡る線としてマッピングする。

これらの方法により構成される情報リストと発生事象のデータを同一画面に表示することにより、発生事象のそれぞれの点と情報リストの距離が直観的にわかる。このことは、比較対象の２つの IP アドレスが厳密には一致しないが、第三オクテッドまで一致している場合などでは、厳密には一致しないが近い位置にあることが視覚的に認識可能となり有効であると考えられる。

次に、発生事象の意味づけを複数の情報リストと比較することにより行いたい場合、インターネット空間の基本パーツを組み合わせることによって観察を実現する(図 5)。例えば、危険なサイトのリストで生成されるインターネット空間と安全サイトのリストで生成されるインターネット空間のそれぞれに発生事象をプロット、あるいは複数の根拠による危険なサイトのリストで構成されるインターネット空間のそれぞれに発生事象をプロットする。そして、これらを並列表示することにより比較が容易になり、発生事象の意味づけが容易になる。あるいは、複数の情報リストで構成されるインターネット空間を並列表示により比較することにより、情報リストそのものの特性を直観的に評価することも容易になる。

図 2. 基本パーツ

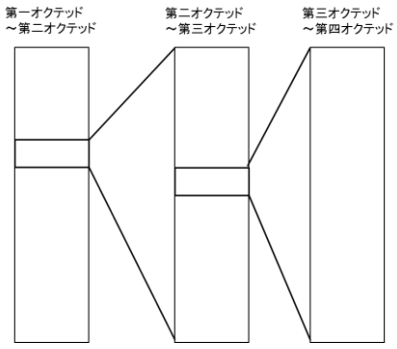


図 3.鳥瞰から詳細化の表示の流れ

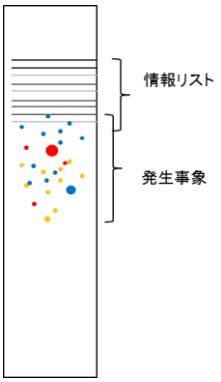


図 4.情報リストと発生事象の比較

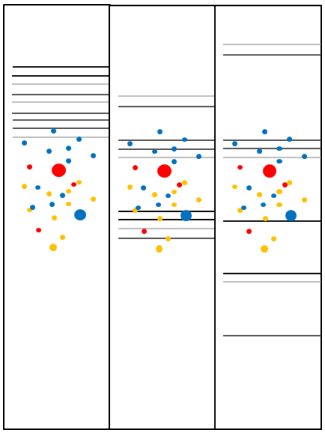


図 5.情報リストどうしの比較

5. 実施例

基本パーツを組み合わせることにより幾つかの実施形態が考えられる。

（１）外部からのアクセスの可視化の例

例えば Web サイトの運営者にとって自サーバへどのようなアクセスがあるのか、攻撃を受けていないか、あるいは攻撃を受けそうなのかどうかが心配になる。このような場合の対応の一つとして、攻撃ログを検出するツールの利用などがある[17]。このようなツールでは具体的な攻撃を検出することができるが、偵察行動や不審な履歴を事前に察知することは難しい。

そこで、Web サイトにおけるログを、通常の正規のアク

Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

セス、ロボットによるアクセス、スキャン、攻撃に分類し、本提案のインタフェースで可視化し観察することにより、攻撃や不審な行動の状況を知ることができる(図 6)。この実施例の場合、アクセスログを事象のあった日付と発信元の IP アドレスによって分割し、日付を横軸、IP アドレスを縦軸としたインターネット空間にプロットする。プロットに際して、事前に把握しているアドレスやアクセスパターン（Web コンテンツへの想定通りのアクセス）であれば正規のアクセスとして分類し、アクセスログ内にロボットであることがわかる項目があればサーチエンジン業者のロボットとし、明らかに攻撃のアクセスパターンの場合は攻撃とし、それ以外はスキャン（または未分類）として分類し、これらの分類に従って色分け表示と、アクセス数の多さに応じてプロットの点を大きさ表現した。これにより自サイトへのアクセスの全体像の時系列の変化を把握することが可能になり、不審なアクセスが増えているかどうか、つまり警戒が必要かどうかを直観的に知ることが可能になる。

また、アクセスの分類においては判定が容易でないものも多く攻撃や不審な行動の判定も難しい。しかしながら、アクセスログを総覧することにより、前後のデータから分類の間違いに気づき修正することも可能になる。特に未分類相当のスキャンについては、このインタフェース表示により、前後のログと比較して観察することにより怪しい偵察行動かどうかなどを補正してゆくことが可能になる効果がある。

（２）内部から外部へのアクセスの可視化の例

次の例として、企業などのネットワーク管理者の立場における利用シーンを考える。ここでは、組織のネットワーク全体のファイアウォールや Web Proxy におけるアクセスリスト(遮断リスト)の設定、管理を担当しているとする。この場合、遮断リストの精査や、遮断リストにおいてアラートとして検出された通信ログからネットワーク内の端末の感染の有無を精査することになる。しかしながらこのような場合、アクセスリストの元となる情報リストの妥当性が不明なため、確実な遮断リストを作るためには、複数の情報リストと通信ログなどを見比べる必要が生じる。

そこで、様々な情報リストと自ネットワークにおける通信ログを同一空間で表示し可視化することにより判断を助けることができる。

そこで、例えば、受信した SPAM メールに含まれていた通信先のアドレスリスト、ネットワークの入口で受信した不審な通信元のアドレスリスト、市販の悪性サイトのリストに対して Web へのアクセスログをマッピングし、それぞれを比較観察することができる(図 7)。このようにすることにより不審な Web アクセスを見つけ出し、それがどのようなリストに該当するのか、あるいはどのような危険な行為に近づいているかを直観的に把握することができる効果がある。

図 7 の例は SPAM メールで受信したアドレスに起因して Web アクセスをしたと思われる例である。なお、アクセス先は悪性サイトとして特に登録されていない。

（３）観察記録のマッピング

観察をするうちに様々なアドレス帯について追加で調査してゆくことや特定のアクセスログに対して追加で調査し知見を得ることがある。そして、繰り返すうちにインターネット空間に対する様々な知見が増えてゆく。一回調べた知見について IP アドレスやアクセスログに紐づけてインターネット空間にマッピングすることにより、観察による知見を蓄積し、次回の調査の際に判断を助けることができるようになる(図 8)。

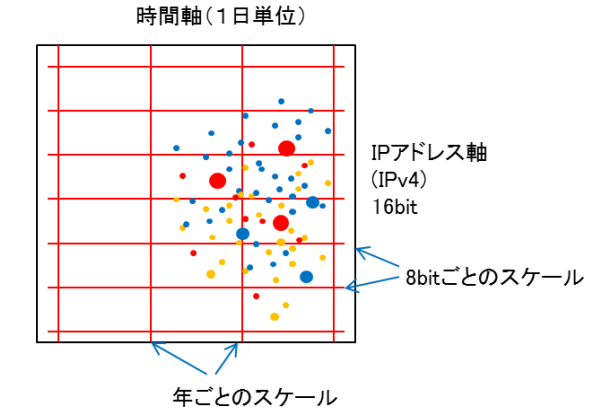


図 6. 表示イメージ 1

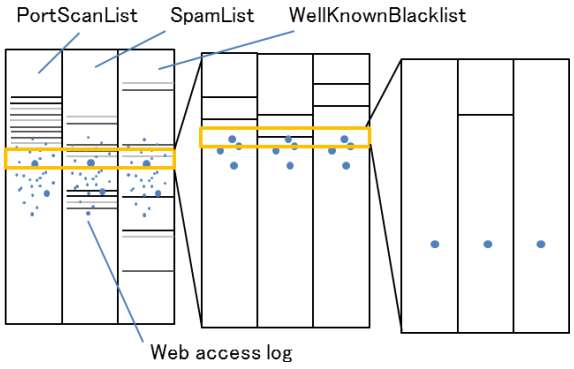


図 7.表示イメージ 2

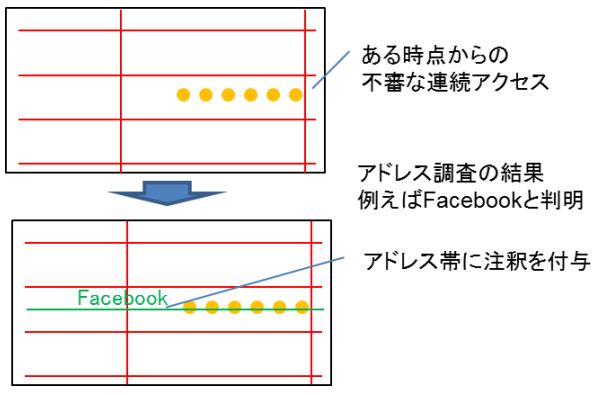


図 8.表示イメージ 3

6. 今後の展開についての考察

今回、IPv4 ベースで通信ログや様々な情報リストをプロットしインターネット空間の状態を、canvas オブジェクトを用い Web ブラウザ上で観察できるインタフェースを提案した。これによりインターネット空間の状況を直観的に把握することができるようになった。仕組みとしては簡単であるが提案方式の今後の展開として次のような 3 つの方向性が考えられる。

（A）観察の有効性
（B）活用シーンに基づいた分析ツール化
（C）セキュリティ観点以外の利用方法

（A）観察の有効性：提案インタフェースによりログを日々観察することにより、新たな動きを発見できる可能性がある。観察対象となるネットワークに対して導入し具体的な効果を測定する必要がある。特に、今回のインタフェースで直観的にアクセス動向がわかったが、これにより組織内ネットワーク内の感染者を抽出できるのか、危険の回避ができるのか、など具体的な効果を明らかにする必要がある。

（B）活用シーンに基づいた分析ツール化：今回のインタフェースは観察用に簡単な表示のみである。実際のオペレーション現場で活用するには、どのような作業を支援するかを明確化し、必要な情報を提案インタフェースに組み込んでいくことになる。例えば、感染しているユーザ端末の特定であれば、提案インタフェース上にユーザ情報やサイト情報をさらに表示させることにより、ユーザ個々の通信先がより具体的に把握できるようになる。ただしこの場合、プライバシー的な観点からも是非を検討する必要がある。またネットワーク管理の現場では、複数人で分析を行うため、ネットワーク管理者どうしのコラボレーションやそれまでに対応した知見の共有という観点を加えた分析ツール化が考えられる。

（C）セキュリティ観点以外の利用方法：セキュリティ上の必要性という観点から IPv4 アドレス空間の可視化を行った。インターネット空間の表示方法としては単純であり特にセキュリティに特化したものではない。このことから、同様の仕組みを利用することにより効果が出る他の利用シーンの有無についても今後検討する必要がある。

7. まとめ

サイバー攻撃に代表されるようにインターネット空間には様々な脅威がある。このような脅威の増加に対して、ネットワーク装置および運用技術として次世代ファイアウォールや標的型対策システムなどの導入などにより、マルウェアの感染防止や感染後の早期発見を行いネットワークを安全に利用するための環境が整いつつある。一方で、普段の利用においてどの程度危険なのか、どのようにふるまえば危険を回避できるのか、について把握する方法が少ない。つまり、感染してから判定されることはあっても、自分自身の利用行動にどのくらい危険性が潜んでいるかを事前に知り回避行動に結びつけることができない。

そこで、IPv4 の IP アドレスに対して、IP アドレスに紐づく様々なサイトの情報リストと、通信ログを IP アドレスと時系列でプロットできるインターネット空間を Web ブラウザ上に構築し、インターネット空間上での動向を観察できるインタフェースを提案した。特に、普段のインターネット利用において危険なアドレス帯にどのくらい近づいているのかを把握することができる。これにより自分自身の利用行動を観察し判断することが可能になる。また、提案インタフェースを用いていくつかの利用シーンについて検討した。

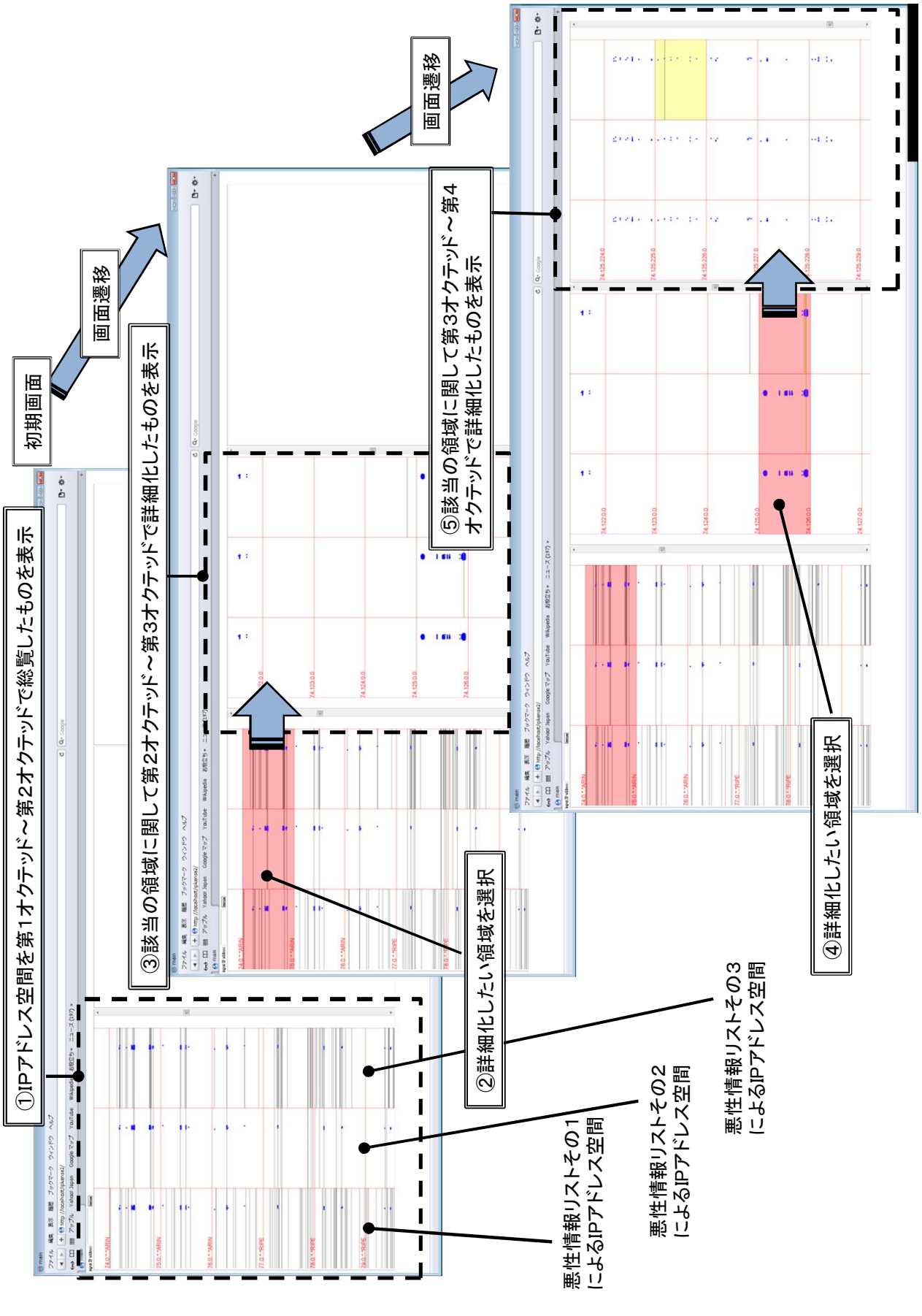
今後の展開として、（A）提案インタフェースを用いてインターネット利用を観察し有効性の検証。（B）実際の活用シーンとしてネットワーク管理者の具体的な作業を支援するための機能を強化した分析ツール化の検討。（C）今回の提案インタフェースは、セキュリティ観点に特化した仕組みではないため、セキュリティ観点に限らず IP アドレスの全空間を可視化し状況をつかむ必要があるその他の利用シーンの検討。などが挙げられる。

参考文献

1) 松野,川村,大久保,小林,高橋,栢口,”新たなサイバー攻撃の出現と今後のセキュリティ研究開発の方向性”,NTT 技術ジャーナル Vol.24 No.8, p.8-12 (2012).
2) http://www.nicter.jp/nw_public/scripts/
3) 千葉,八木,秋山,森,後藤,”多種多様な攻撃に用いられる IP アドレス間の相関解析”,CSS 2011, p.185-190 (2011).
4) http://maps.measurement-factory.com/
5) RSA CyberCrime Intelligence Service http://japan.rsa.com/node.aspx?id=3977
6) https://www.paloaltonetworks.com/
7) 笠間,中里,鈴木,衛藤,井上,中尾,秋山,青木,岩村,八木,斉藤,針生,”多様なセンサの観測情報を用いたマルチモーダル分析”,SCIS2012 2E3-4 (2012).
8) 笠間,中里,衛藤,井上,中尾,秋山,岩村,八木,斉藤,針生,”マルウェアの攻撃プロセスに着目したマルチモーダル分析”,SCIS2013 3D3-4 (2013).
9) http://www.aguse.jp/
10) http://www.siteadvisor.com/sites/
11) https://safeweb.norton.com/
12) http://jp.sitesafety.trendmicro.com/
13) http://www.google.com/transparencyreport/safebrowsing/
14) http://check.gred.jp/
15) http://www.urlvoid.com/
16) http://www.ipvoid.com/
17) http://www.ipa.go.jp/security/keihatsu/pr2012/tech/031_ilogscanner.html

Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

Appendix 1



Vol.2013-DPS-156 No.29
Vol.2013-GN-89 No.29
Vol.2013-EIP-61 No.29
2013/9/13

Appendix 2