

## 集合知を用いたセキュリティシステムの提案

祢宜 知孝 河内 清人 藤井 誠司<sup>†</sup>

三菱電機株式会社 情報技術総合研究所<sup>\*</sup>

### 1. はじめに

本稿では、集合知の考え方を用いたセキュリティ情報収集・共有システム(以降、集合知セキュリティシステムと呼ぶ)を提案する。集合知をセキュリティ情報として用いる為には、解決しなければならない課題が存在する。そこで本稿では、課題を指摘すると共に、解決する方法の提案を行い、システムコンセプトやシステム構成、及び実現上未解決の課題について述べる。

#### 1.1. 背景

近年、ブロードバンド化が進み、ゲーム機や家電、各種情報端末、携帯電話までもがインターネットに接続され、インターネットが日進月歩で巨大化している。今やインターネットは個人に非常に身近な存在となっている。一方、攻撃者の目的は、悪戯目的から金銭目的へと変わると同時に、その攻撃手法や攻撃対象が多様化し、誰もが様々な脅威に晒されるようになった。

そこでユーザを脅威から守る為に、(1) IPA<sup>1)</sup>やJP-CERT/CC<sup>2)</sup>、各セキュリティベンダから脆弱性情報やマルウェアに対する注意喚起、インシデント情報等のセキュリティ情報が提供されている。また、(2)スパムメールをフィルタリングする Spam Assassin<sup>3)</sup>等、特定の管理者によって管理されるブラックリスト形式のセキュリティ情報が提供されている。その他、(3)インターネット上には個人や閉じたコミュニティによって有害サイトのURLや迷惑電話発信元等に関する情報がセキュリティ情報として提供されている。

しかし、上記の(1)～(3)のセキュリティ情報にはそれぞれ問題がある。(1)と(2)に対する問題点は、特定機関によって情報の収集が行われており、情報が公開されるまでに時間がかかる点である。(3)に対する問題点は、情報の信頼性を担保されていない点及び、発信元が散在しており、多くの人々に知られていない点である。そこで、ユーザ全員が参加可能であり、情報が即座に多くの人に行き渡り、信頼性が担保されたセキュリティ情報を提供する事が可能な仕組みが必要である。

#### 1.2. 既存の問題点

我々は Web2.0 の一要素である集合知(フォークソノミ:Folksonomy)に着目した。ソーシャルタギングやウィキペディア<sup>4)</sup>のようなインターネット上で公開・作成されている多言語の百科辞典などがフォークソノミの代表的な例である。多数のユーザがセキュリティ情報を通報・共有することによって、インターネット上の脅威から身を守る方法(図 1)が考えられる。しかし、フォークソノミには大きな課題が存在する。それは、フォークソノミの考え方自体が、性善説に基づいており、悪意を持ったユーザは存在しないと言う点である。

実際には悪意を持ったユーザが存在し、偽情報の書き込みや情報の削除・改竄などを行っている。つまり、前述した(3)のセキュリティ情報と同様の問題点が残されている。これは、主として情報の書き込み・修正・削除等

を匿名で行える事に起因する。しかし匿名性を完全に排除してしまうと、プライバシーの問題が生じてしまう。その為、適度に匿名性を維持しつつ、各ユーザの情報操作を追跡可能とする事によって、悪意を持った情報操作を減らす事が必要である。

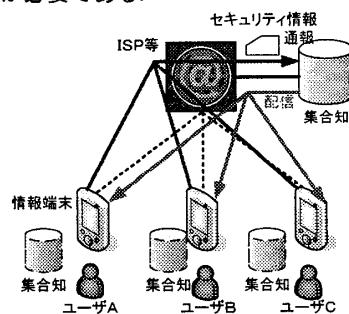


図 1. セキュリティ情報の通報・共有

### 2. システム提案

そこで、下記の特長を有した集合知セキュリティシステムを提案する。

1. 事後証跡可能な情報(ユーザ ID 等のユーザ情報)を用いることによって集合知セキュリティサービス提供者のみがユーザを特定できるようにする事で悪意を持ったユーザによる偽情報の通報を防ぐ。
2. 事後証跡可能な情報(ユーザ ID 等のユーザ情報)の付与を義務化しない事により情報の提供者が誰であるか誰も特定できない完全匿名をも可能とする。
3. 「集合知中のセキュリティ情報がどれだけ信用できるか」を示すセキュリティ情報信頼度と「セキュリティ情報を提供するユーザがどれだけ信用できるか」を示すユーザ信頼度の概念を導入する。そしてセキュリティ情報信頼度とユーザ信頼度に相関関係を持たせる事によって悪意を持ったユーザによる偽情報の提供を防止する。

#### 2.1. 基本動作

ユーザはユーザ情報と共にセキュリティ情報を集合知として集積・共有する方法を基に、前述の特長を有して、セキュリティ情報を通報する際にユーザ情報を付与する事により、通報するセキュリティ情報に対してユーザが責任を持つ。さらに、ユーザは、自分が通報した情報を元に自分を評価されるため、精度の高い情報を ISP やキャリアに通報する事になる。以降では、どのようにセキュリティ情報信頼度とユーザ信頼度に相関関係を持たせるかに関して詳しく述べる。

ゲーム機や家電、各種情報端末、携帯電話は、インターネットに接続するために必ず ISP や通信キャリアにアクセスをする為、必ずユーザ情報に相当するユーザアカウントや USIM(Universal Subscriber Identity Module)を保有している。そこで、ユーザが新しくセキュリティ情報を発見した時やセキュリティインシデントに遭遇した際には、セキュリティ情報と共に、ユーザ情報を ISP

Study of the Security System with Folksonomy Technology

<sup>†</sup> Tomonori NEGI, Kiyoto KAWAUCHI, and Seiji FUJII

<sup>\*</sup> Mitsubishi Electric Corporation Information Technology R&D Center

や通信キャリアに設置された集合知 DB に通報する。セキュリティ情報の通報を受けた ISP や通信キャリアは、以下のルールに基づいて、通報されてきたセキュリティ情報に対してセキュリティ情報信頼度を付与する。

- ユーザ情報を付与して来ており、且つ年齢、性別などの個人情報を利用する事に合意をしているユーザから通報されて来た場合には、ユーザの過去の通報履歴を基に算出されたユーザ信頼度に信頼度 $[v]$ を加算した値をセキュリティ信頼度として加算する。この時値 $v$ もユーザの過去の通信履歴を元に増減する。
  - ユーザ情報を付与して来ているが、個人情報の利用に合意していないユーザから通報されて来た場合には、ユーザの過去の通報履歴を基に算出されたユーザ信頼度に信頼度 $[v(v)]$ を加算した値をセキュリティ信頼度として加算する。この時値 $v$ もユーザの過去の通信履歴を元に増減する。
  - ユーザ情報を付与して来ていない場合には、固定値 $[v]$ をセキュリティ信頼度として加算する。
- また、ISP や通信キャリアは、以下のルールに基づいてユーザ信頼度を算出する。
- 過去に通報して来た履歴がないユーザに対しては固定値 $[x]$ をユーザ信頼度とする。
  - 一定期間内にある一定以上の信頼度 $[v]$ に達したセキュリティ情報を提供してきたユーザに対しては固定値 $[y]$ を加算する。
  - 連続的に一定期間内にある一定以上の信頼度 $[v]$ に達しなかったセキュリティ情報を提供してきたユーザに対しては固定値 $[z]$ を減算する。

そして、各ユーザは、集合知 DB に蓄積されたセキュリティ情報とセキュリティ情報信頼度を用いて様々な脅威から身を守る。

## 2.2. システムの全体像

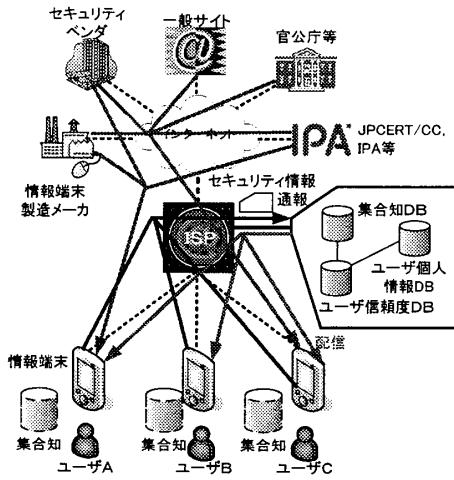


図 2. システムの全体像

図 2 は、本稿にて提案する集合知セキュリティシステムの全体像である。各情報端末は、ISP や通信キャリアの集合知データベースからセキュリティ情報を集合知として受信する他に、各ユーザによって予め設定されたサイト（情報端末メーカやセキュリティベンダ、JPCERT/CC など）からセキュリティ情報を収集する。各ユーザは、情報端末にセキュリティ情報収集元サイトを設定する際に、各サイトの信頼度を設定する。例えば、ユーザ C は、情報端末製造メーカやセキュリティベンダ、官公庁、

JPCERT/CC に対しては信頼度を 100%に設定し、一般サイトに対してはサイト毎に 1~100%の範囲内で任意に設定する。ユーザが一般サイト毎に信頼度を設定する事によって、玉石混交のサイトから提供される情報に対して、信頼度の精度を向上させる事が可能となる。そして、新たなセキュリティ情報を発見した時や、セキュリティインシデントが発生した際には、2.1で述べた仕組みによりセキュリティ情報の収集や共有がなされる。また、ISP や通信キャリアは、本稿で提案した集合知セキュリティシステムをユーザに積極的に利用してもらい、且つユーザ情報を積極的に提供してもらうために、「ユーザ情報を付与して来ており、且つある一定期間内にある一定以上の信頼度に達したセキュリティ情報を提供して来たユーザ」に対しては、マルチメディアコンテンツの無料ダウンロードなどのインセンティブを与える。

### 3. おわりに

以上、適度な匿名性を維持しつつ、セキュリティ情報をユーザ間で共有する事が可能な集合知の考え方を用いたセキュリティシステムを提案した。しかし、本システムにはまだ解決すべき課題が残されている。以下に解決すべき課題を列挙し、纏めとする。

- 1) 「マルウェアや SPAM、SPLIT、有害サイト、不正サイトを特定するためのセキュリティ情報として何が適切であるか？」

特にマルウェアはステルス化しており、ユーザが気付かないケースが増えてきているので、マルウェアと思われる物に対して情報端末が自動的にセキュリティ情報を送信する仕組みが必要と思われる。

- 2) 「各情報端末が集合知を如何に取得するか？」

情報端末の中には、記憶容量の少ない機器も存在し、集合知 DB の全情報を保有できない可能性がある。そこで、情報端末が集合知 DB のミラーを保有するのか、ISP やキャリアにある集合知 DB を検索するかを検討する必要がある。さらに、情報端末が集合知 DB のミラーを保有するとしても、ISP やキャリアがブロードキャストで配信するのか、情報端末が ISP やキャリアに取得しに行くのかを検討する必要もある。

- 3) 「現在の基本コンセプトでは、セキュリティ情報が通報される度にセキュリティ情報信頼度を上昇させるのみであるが、セキュリティ情報信頼度を下降させる仕組みは必要ないのか？」

下降させる仕組みが必要なケースの有無や状況を検討する必要がある。

- 4) 「蓄積された集合知を集合知 DB に蓄積し続けて行くのか、それともある時点で集合知 DB から削除するのか？」

また、ある時点で集合知 DB から集合知を削除するのであれば、どのタイミングで削除するのかを検討する必要がある。

- 5) 「収集された集合知の検証は必要ないのか？」

検証するにしたら、如何に検証するのかを検討する必要がある。

上記の課題は、互いに関連しあっているため、慎重に検討し、解決する必要がある。

1) <http://www.ipa.go.jp>

2) <http://www.jpcert.jp>

3) <http://spamassassin.apache.org/>

4) <http://wikipedia.org/>