Sentinel Protocol

ブロックチェーンのセキュリティインテリジェンスプラットフォーム (SIPB)

要旨

21世紀におけるコンピューター技術の目まぐるしい発達は、さらなるイノベーションの前に立ちはだかる知的で洗練された脅威の存在を明らかにした。仮想通貨の本質が分散化にある一方で、その分散化が最大の弱点となっている。分散型の仮想通貨のシステム上、脅威に対して防衛するシステムが存在しないため、セキュリティへの負担はこれまですべて個人や企業の肩の上にあった。Sentinel Protocolは分散化の不利益を、セキュリティを考える上での優位性に変えることでそれを克服する。分散化の力を最大限生かすことで完成する集団的知性のシステムを利用することで、Sentinel Protocolは安全で革新的なエコシステムを創り上げるために暗号学的機能と知能ベースの脅威分析アルゴリズムを結合させた。

Uppsala 財団

2018.04.07

チャプター1

序論

仮想通貨の技術の根幹であり、イデオロギーとして働く分散化は、技術革新であると同時に先天的な不安をもたらす。この革新と不安は自律性に起因する。匿名性を土台とした自律性はシステムにのしかかる莫大な責任によってのみ達成することができる。現実を見ると、上述の匿名性を土台とした自律性の副作用は無数のサイバー犯罪の実例の中でも最も明らかである。その上、サイバー犯罪から人々を守るための根本的な防衛システムはまだ存在しない。

一般的な仮想通貨を利用するユーザーは主に3つのセキュリティに関しての問題に直面している。第一にこれらの一般ユーザーがハッキングのリスクにいとも容易くさらされていること。第二に攻撃側がターゲットを特定することができる一方で、我々はハッカーを特定できない点。最後にハッキング被害の損害はすべて我々ユーザーの責任としてのしかかる点。一体どのようにしてこれらの問題を解決することができるのか? 結局、責任を持つのはすべて我々ユーザーである。しかしながら、個人が仮想通貨のセキュリティに対しての問題解決を図ったところでそれが解決策とはなり得ない。そこで、分散型のサイバーセキュリティのエコシステムを通じて、それぞれが相互の自己利益のために共に動くことを可能にする私たちが開発した集団的知性を利用していく必要がある。我々の分散型のAIシステムは、根本的な分散化の自律性を守りつつも、攻撃者の未知なるパターンを検出、エコシステム内に拡散、そして集団的知性を利用することですべてのメンバーを守ることを可能にする。

チャプター2

問題提起

一般的に、セキュリティ脅威に対しての個人ユーザーとビジネスユーザーの対策レベルの違いは実にシンプルである。技術や人材にどの程度の予算を投入することができるか? という違いだ。この事実に対する客観性を上げるために、SANS institute(*1)のITセキュリティに関しての支出調査を参照する。2016年、金融機関は50万ドル～100万ドルの年度予算のうち平均10～12%をITセキュリティに充てている。次点の政府系の取次は100万ドル～1000万ドルの予算の7~9%、教育やヘルスケアなどの他の産業はこれより小さな数字となっているが、安定した割合でセキュリティへの支出を増やしている。Cybersecurity Ventures(*2)からの報告によれば、増加し続けるサイバー犯罪の件数が、致命的なレベルを超えていることからも、2017年から2021年にかけて、サイバーセキュリティの市場が1兆ドル規模で拡大することが予想されている。

ここで、法人ユーザーが多くの専門家やセキュリティに関するソリューションに守られている一方で、エンドユーザーは自身を守るためにどのような手段をとらなければならないのかという点に注目する。不運にも、彼らが最善を尽くしたとしても、品質の悪いソフトウェアやハードウェア、個人としての専門性の欠如から逃れることはできない。ブロックチェーン技術が進化していくと同時に、様々な詐欺やサイバー犯罪もまた発展している。ユーザーのデータを人質に取り、その解放の代償としてビットコインなどの金銭的な補償を要求する新たなタイプのものは、最もよく知られているサイバー犯罪の一つであるランサムウェアと呼ばれる。このランサムウェアの市場は2021年までに173.6億ドルまで膨らむことが予想されている。恐らく、ビットコインはサイバー犯罪において、その金銭的価値故にサイバー犯罪における通貨として選択されるという皮肉めいた状況の渦中にいると言えるだろう。

2016年のDAO事件はブロックチェーン時代において初めてのセキュリティの脆弱性を突かれた大規模な事件で、コードの脆弱性が為にすべてのイーサリアムの15%がハッカーの攻撃に晒されることになった。そのため、数万もの投資家が財政的な損失に苦しめられる結果となった。この問題を解決するための唯一の方法はハードフォーク(*3)を行うことであったが、それはブロックチェーンの不変性という哲学的な信念に反するものとなった。断固とした分散化の難しさ、また長い間自己責任として一蹴されてきた強い自律性がこの大惨事の根源には眠っている。

Chapter 3

分散化におけるセキュリティ

近頃は、誰もが最低一つのメールアドレスを所持しており、名刺にメールアドレスが書かれていないという状況を想像するのは極めて困難である。しかしながら、この皆が共通でもつ常識こそが脆弱さとなり現れている。ワードやエクセルなどの添付ファイルに悪意のあるマクロなどを仕組むフィッシングのケースだが、これ感染した添付ファイルを開くことでユーザーのコンピューターを感染させる。2017年7月、韓国の大手仮想通貨取引所であるBithumbは感染したファイルを開きハッキングを受け、31,000の顧客の秘匿情報が盗まれる事態に陥った。また、このフィッシングを仕掛けた犯人は依然として特定できていない。

フィッシングはEメールに限られたことではない。電話を利用したテレフォンフィッシングにおいては、仮想通貨取引所の管理者を装った人物がユーザーを欺き、個人情報を奪い取ったケースなど様々な手段が確認されている。例として、管理者を装った人物がユーザーに対して、取引所がハックされたのでパスワードをリセットするために個人情報が必要であると伝えそれを要求する。ユーザーの心理的な弱点を利用・搾取し、ハッカーはアカウントへのアクセスを得る。

別の形の詐欺はICO(Initial Coin Offering)にて散見される。ユーザーに対して偽のICOの資金集めのプラットフォームを提供、或いはオリジナルのICOのウェブサイトをハックしアドレス部分のみを書き換えるなど、様々な手口が横行している。

これらの様々なハッキングの手口におけるキーは、インターネットのオープンな性質上ユーザーがあまりにも標的にされやすいことだ。仮想通貨とインターネットの双方において分散化のイデオロギーは不可欠なものになってくるが、ブロックチェーンが完璧な自律性を実現すると断言することは決してできない。オープンな状態にある自律性は須らく自己の責任と隣り合わせにある。分散化はすべての問題における解決策ではないし、我々はインターネットを利用する人々が皆善人であるような幻想の世界で生きているわけではない。現実を見なければならない。悪人は常にインターネットのこのような性質を利用している。ゆえに、分散化にとってのイデオロギーはセキュリティという哲学を発達させていく必要がある。

チャプター4

ブロックチェーン上の評価システム

ビットコインの根幹にはブロックチェーン(*4)と呼ばれるシステムがある。これは完全なるP2Pシステムで中央管理者のコントロールを必要としない代わりに合意形成のアルゴリズムを用いて完成する。個人同士での信用がない状態でも、この合意形成のアルゴリズムによって送金が完了する仕組みである。この決済のプロセスにおいて、すべてのトランザクションが記録されシェアされるというルールが存在する。しかし、現実におけるこの金融商品の商業化は、技術的な側面は差し置いても、個人の資産などの情報がすべて可視化されてしまう点で難しい。他方で、個人情報の保証抜きにしては、数ある金融サービスに参入することも難しく、また時間が経過するにつれてルールや規制などもより厳格になっていくだろう。パブリックのブロックチェーンの利益のすべてを享受することはできないものの、その一つの代替案にコンソーシアムブロックチェーンが挙げられる。

パブリックな分散化の利益を引き継ぐ最良の解決策は何であるかという根本的な問いは、情報がすべて公開・蓄積された際に、それがより価値のあるものとなるかどうか? という問いに置き換えることができる。

仮にブロックチェーン上での評価システムと現在起こっているサイバー犯罪に関する情報すべてがブロックチェーン内で共有されたとすれば、ブロックチェーンの分散型のシステムによって大衆を守ることが可能となる。既存の評価システムの問題点は情報の操作や改竄が可能である点にある。個人や悪意のあるグループが組織やシステムの評価を操作、または記録されている評価を操作するためにブロックチェーン上のシステムをハックしようとする際、後者の場合はブロックチェーンのデータ整合性によって自然に解決される。しかしながら、トランザクションではなく情報の質を記録する評価システムにおいて、シビル攻撃などの攻撃に対しては、ブロックチェーンの基本的な特性のために対策を行うことは容易ではない。なぜなら、いかなるトランザクションの評価にかかわらず、事前に操作された情報の主観的な性質によってそれらを記録させてしまう可能性があるからだ。しかし、集団的知性の力を使うことでこの問題は解決される。

チャプター5

集団的知性

サイバー犯罪と聞くとブロックチェーンの悪用というイメージがあるが、ブロックチェーンにはレジャーの分散・共有によってこういった犯罪を未然に防ぐという優位性もある。さらに重要なのが、捜査のフレームワークを作ることが可能ということである。例として、サイバー犯罪を行う人々はブロックチェーンの構造上ユーザーの情報を盗み取ることができないという偏見があるが、これは大きな間違いである。

本質的にはブロックチェーンはすべての情報を透明に共有するシステムである。すべてのトランザクションは分散型のレジャーに記録され、特別なパーミッションなしで認証される。この仕様によって、すべてのトランザクションを追跡することが可能になる。実際、サイバー犯罪における仮想通貨のトランザクションの経路は容易に追跡することができる。しかしながら皮肉なことに、その追跡を避けるための最も一般的な方法として、仮想通貨取引所やコインを両替するシステム利用した資金洗浄が挙げられる。コインを両替しなければその価値は失われる性質のために、ここに善循環が生まれる。たとえ、トランザクションの情報を隠すことのできる匿名通貨、Dash，Zcash，Moneroを利用したとしても両替ができなければその価値は失われる。これらのコインの追跡可能性を高めることは、ICF(相互協力フレームワーク)はBlockSci(*6)などのトランザクション分析プロジェクトと協力することで達成することができる。

また、サイバー犯罪に関しては、各国の仮想通貨の取引所と協力することも不可能ではない。彼らもまた、厳しい規制の中でユーザーを守るために努力をしている。同時にこれは、多くの仮想通貨取引所が、ユーザーの個人情報を守るという基礎的な義務を果たすために、警察や政府の捜査機関の同意の範囲内ですべてを行う必要があることを示唆する。しかし、各国で異なる法律の下で、仮想通貨の専門家が様々な国のこういった法律に合わせたセキュリティの対策を協力することは非常に難しい。更に、多くの国が仮想通貨絡みのサイバー犯罪を、現実の金融犯罪と同等に扱っていない状況である。結論、法に拘束されたシステムによって苦しむのは善人のみである。

分散型の捜査システムへの障害となっている既存の法システムに存在する巨大な穴を埋めることができるのは、改変不可能なデータベースの中に、存在し、今もなお起こっているすべての疑わしいサイバー犯罪の情報を持つブロックチェーン自身だ。すべての情報を、個人、取引所、プロジェクト、セキュリティ会社、政府に即座に透明に提供することができる。それだけでなく、世界中の人々によって、一つのシステムの中でこれを共有、追跡することができるのだ。評価システムもまた、集団的知性によって管理されるが、これによって同時にシンプルさをもたらす。このシステムによって、取引所は複雑な法的根拠などを参照する必要性なしにシステムの評価を信頼することで、先進的なアクションをとることができる。こうして、仮想通貨産業の内にはびこる多くのサイバー犯罪を防ぎコントロールすることが可能になる。多くの専門家から徹底的に承認され認められた人々や機関のみが、この分散型捜査システムを維持することができる。

チャプター6

人工知能

人工知能を利用するメカニズムは、最適なアルゴリズムを用いて良質かつ大量のデータをシンプルに組み立てることである。攻撃者は個人、グループ、政府、企業や組織をターゲットにする際、システムの脆弱性を利用するために長い時間をかけて予期せぬ数の攻撃を上手に操る。その後、コマンドとコントロールコミュニケーションチャネルがハッカーの外部のコマンドタワーと共に創り上げられる。内部のネットワークに既に入り込んでいるハッカーの挙動を掌握することは簡単なことではない。多くのセキュリティ技術は、一見もっともらしく見える集合体の挙動を疑い、正確に二進数で攻撃のサインであると表示する術を備えていない。この理由から、多くの攻撃は通常のユーザーの挙動であると認識されてしまう。

少し、バッタとハリガネムシに関しての話をしたいと思う。ハリガネムシは自らが湿地でしか繁殖できないのにもかかわらず、バッタや他の陸地に生息する昆虫に寄生する。寄生されたバッタは、はじめは正常なバッタと何ら変わりない動きを見せる。しかしながら、ハリガネムシの繁殖の準備が整うと、バッタの挙動に変化が生じ始める。化学物質の分泌により、ハリガネムシはバッタの精神をコントロールし水場へと向かわせ、バッタはその結果溺死という形で自殺をする。こうして、ハリガネムシは出現し、新たなライフサイクルを始めることができる。

機械学習のセキュリティ技術において鍵となるのは、見かけによる変化ではなく挙動における変化の追跡をすることができる点である。ハリガネムシはバッタの頭脳をコントロールする一方で、バッタは外面的には通常で健康であるにもかかわらず、水場を探し求めるなど、典型的な活動において通常の範囲外での挙動を見せる。この不自然な挙動の観察のみによって昆虫学者はバッタが感染しているということを判断できる。同様に、見かけの変化ではなく目立たない挙動における変化との相関関係に注目すれば、特に何も起きてない状態であっても、我々はそれを実証的なリスクとして事前に認識できるうえ、被害を防ぐ高い可能性を得ることができる。

Sentinel Protocolがブロックチェーンと人工知能を共に利用する方法は二通り存在する。第一には、機械学習をベースとしたクライアント向けブロックチェーンセキュリティウォレットで、それはユーザーやノードの情報を集め、すべての側面、例として通常のコンピューターの使用パターン、トランザクションのパターンなどから挙動のモデルを作成する。疑わしい挙動が検出されれば、セキュリティウォレットが脅威の可能性としてそれを認識し、プロセスの実行をブロックする。これに関しての詳細な情報は集団的知性のグループへと報告され、評価システムに共有される。すべての情報はAPIによって利用したいユーザー全員へと共有される。これは世界でも最も正確でセキュアな世界規模の知能システムへと拡張される。

第二には、ブロックチェーンのデータを利用した、詐欺検出システムを構築することである。本質的に、Sentinel Protocolの異常検出は合意形成アルゴリズムと紐づけされている。専

門家により選び抜かれた(或いはUppsalaがSIPBの初期段階で選抜した) 集団的知性のグループまたは個人が、Sentinelと名付けられた、国際サイバー犯罪警察として働く。彼らは研究や分析に関しての責任、また評価のシステムを更新する権限を持つ。これに対しての報酬はSentinel Protocolの経済システムによって支払われる。更には、インサイダー的な脅威を押さえるために詐欺検出システム(FDS)が搭載されており、これによって通常のユーザー同様、集団的知性に対しても、通常とは異なる挙動を監視、検出することができる。

チャプター7

セキュリティの特徴

Security Intelligence Platform for Blockchain(SIPB 或いは Sentinel Protocol)は以下のユニークな特徴を持つ。

- 脅威評価データベース(TRDB)
- 機械学習エンジン統合型セキュリティウォレット(S-Wallet)
- 分散型マルウェア分析サンドボックス(D-Sandbox)

脅威評価データベース(TRDB)

脅威評価データベース(TRDB)は既存のサイバーセキュリティ産業の二つの問題に対して機能する。第一の問題は、セキュリティ会社の集権的なデータベースである。脅威に関しての情報を一つの集権的な場所に置いておくことは情報を操作や悪用に対して脆弱にさせる。データベースはたちまちシビル攻撃、サーバーのハッキング、またはサービスの妨害などの明確なターゲットとなる。これは、インターネットの集権的なクライアントサーバーモデルの根本的な問題である。2017年11月、ロシアの国のハッカーがカスペルスキーという有名なセキュリティ会社のソフトウェアを使ってNSA(アメリカ国家安全保障局)の情報を盗み出した例がある。基本的に、ハッカーはセキュリティツールを用いて標的の脆弱性を見つけ出していた。ブロックチェーンが持つ分散型の性質は、データの改ざんを難しくする不変性のためにそれらの問題を和らげることができる。これにより、データを提供するサーバーのセキュリティ面での安定性が高まる。

もう一つの問題は、セキュリティベンダー間で共有されている知識の不足である。集められたリスクに関しての情報が多ければ、それだけサイバー犯罪を防ぐことのできる確率も高くなる。しかしながら、それぞれのセキュリティベンダーは、勝者が全てを手に入れるが如く脅威に関しての情報をそれぞれで集めている。なぜなら、ベンダー同士が協力し一つの包括的なデータベースを作ることに何もインセンティブが存在しないからだ。ガートナーの研究VPであるAnton Chuvakin氏はかつて『悪人がデータやトリック、手法などを共有している一方で、善人がそれを行う術を持っていないことは非常に悔やましいことだ』と語っていた。この大きな非効率性に対価を支払うのは一般の人々である。善意単体ではスケールすることができない。したがって、チャプター11に説明されるTRDBはインセンティブスキームを利用することによってこれを可能にする。セキュリティの専門家やベンダーは合意形成メカニズムと参加者のフィードバックの元で脅威のデータベースの構築に貢献することを推奨される。これをDelegated Proof of Stake(DPoS)と呼ぶ。集団的知性を通じて、TRDBはいくつか例を挙げるのであれば、ハッカーのウォレットのアドレス、悪意のあるURI、フィッシングアドレス、マルウェアのハッシュなどを最も効率よく、効果的に集めることができる。

TRDBは誤検知などのシステム的なエラーを除去するため、セキュリティの専門家によってのみ更新される。一般のユーザーもこれに参加することはできるが、これには自動報告と手動報告という二つの方法が利用される。仮にユーザーが自動報告を許可すれば、機械学習エンジン統合型セキュリティウォレットによって自動的に検出された未知の脅威はデータベースへと

運ばれる。手動報告の場合、ユーザーはリスク情報を報告することができるが、これはコミュニティによって後に承認される。TRDBはAPIとして提供されるので、いかなるユーザーや機関(仮想通貨のウォレットのプロジェクト、取引所、セキュリティベンダー等)でも情報を利用することができる。

機械学習エンジン統合型セキュリティウォレット(S-Wallet)

S-Walletはウイルス対策ソフトの機能性を持つ。しかしながら、基本的な違いはというと、ウイルス対策ソフトはすべての既知の署名に対して集権的なサーバーを介して最新のアップデートを受け取ることによってのみ、新たな脅威に最大限対応することができるという点である。このアプローチではゼロデイ攻撃などの未知の脅威に対応することが難しい。一方でS-Walletは脅威の傾向や履歴を、ゼロデイ攻撃などの未知の脅威に積極的に反応するために解析する。そのため、S-walletは署名による更新を必要としない。この監督者不在の学習アプローチはランザムウェアなどの脅威に対して特に有効である。S-WalletはTRDBと接続し集団的知性をうまく利用することができる他、以下の情報ブロックのサービスを提供する。

- 仮想通貨ウォレットアドレスフィルタリング
- URL/URIフィルタリング
- データフィルタリング
- 詐欺検出システム

ここで理解すべき重要な点は、機械学習の技術によってすべての分散型レジャー上の詐欺検出システム(FDS)を利用可能にし、誤用或いは盗難の報告がなされたトランザクションを特定することだ。これによって、二次的な被害を最大限防ぐことができる。

分散型マルウェア分析サンドボックス(D-Sandbox)

サンドボックスとは、セキュリティメカニズムの一つのことで、アプリケーションやホストへのリスクなしに、未確認・未承認のプログラムやコードを隔離された仮想マシン上で検査することができるメカニズムである。D-Sandboxには潜在的な脅威がチケットシステムを介して提出され、これが集団的知性を用いて解析される。

D-Sandboxは二つの非常に優れた特徴を持つ。第一に、コストパフォーマンスが著しく高い点。分散型のシステムを利用することで、限界のないスケールが保証される。通常のサンドボックスを利用したセキュリティアプライアンスは、仮想マシンを動かすために割けるリソースによって制約されていた。コストの高いセキュリティアプライアンスでさえ、この通常のサンドボックスを利用する方法によるマルウェアの分析は非常に限定的であった。更に、通常のサンドボックスは期待以上の高い処理能力、バンド幅、用途を保証することができなかった為、非常に不安定であった。これがしばしばシステムパフォーマンスの低下や誤作動を引き起こし、ユーザーエクスペリエンスを害するだけでなくマルウェアを感染させる結果をもたらした。

第二に、D-SandBoxはProof of Work(PoW)のアルゴリズムを採用することで、計算能力の無駄を省くだけでなく、よりよいセキュリティのエコシステムを築き上げることに成功した。

確かに、ハッシュ値を生み出すだけの計算能力を利用することは他でもなく無駄である。Sentinel Protocolのネットワーク上に参加しているノードは、彼らの計算能力を使って追加でマルウェアの分析をすることができる。結局のところ、分散型のシステムの優位性は、動いていないリソースを必要な場所に割り当てることができる点である。個人ユーザーが仮想マシンを通じてサンドボックスを提供することで、全体のセキュリティのエコシステムを引き上げることが可能になる。

チャプター8

Sentinel Protocolのエコシステム

以下はSecurity Intelligence Platform for Blockchain (SIPB或いはSentinel Protocol)エコシステムにおけるユースケースの解説である。

相互協力フレームワーク(ICF或いはSentinel Portal)

仮想通貨産業におけるビジネスの継続性の最大の障害の一つがセキュリティである。顧客のハッキング事件やその周辺コストは、近頃莫大な増加を見せているが適切なセキュリティ対策は依然としてとられていない。確かに、産業の成長の速度が早ければすべてのセキュリティ要素をもれなくカバーすることは難しくなるが、これは言い訳であるべきでない。仮想通貨取引所のプラットフォームの中には、初期段階のシステムデザインから、本格的な操業までセキュリティの専門技術を欠いているケースもある。カスタマーサービスの専門家はサイバー犯罪のスペシャリストになることはできないが、現状彼らは二足の草鞋を履いている状態だ。Sentinel Protocolは信頼できる仮想通貨のセキュリティ専門家と集団的知性によって成り立つ本質的なフレームワークを提供することでこの問題を解決する。Sentinel Protocolのコミュニティに参加するだけで、仮想通貨のユーザーは簡単に知識を得てすべてのセキュリティの問題におけるサポートを受けることができる。また、Sentinel Protocolによって提供されるセキュリティのソリューションをデプロイすることも可能である。これによってビジネスと個人ともに非効率なコストは削減される。このフレームワークによって仮想通貨の全体のセキュリティが向上し、分散化の基礎的な原理のもとでより反映することになるだろう。

ベータ版のアナウンスはこちらで予定されています：https://www.sentinelprotocol.io

犯罪防止システム

仮想通貨の現実社会への適用が進んでいく一方で、仮想通貨資産の整合性を検証するシステムは存在しない。これは、ハッカーが盗んだ資産を分割し混合させる以上、盗まれた資産が商業サービスにおける決済で乱用される可能性があることを示唆する。現実社会でクレジットカード会社による、盗難カードの利用制限同様、Sentinel Protocolはすべての盗まれた資産を追跡しこの情報を仮想通貨のサービス提供者に共有する。それによって、盗まれた資産は法定通貨への交換ができなくなる。この防衛スキームは仮想通貨を規制の制約のもとに保護する形となるだろう。

不正トランザクション防止

詐欺と登録されたアドレス、またそこから派生するアドレスは、ブロックチェーンの性質の為に、Sentinel Protocolのコミュニティ内にすべてリアルタイムで共有される。Sentinel Protocolが適用されている限りは、更なるダメージの拡大を防ぐことができる。この適用可能な利用法の一つに、ICOが挙げられる。ICOは短期間で多くのユーザーが参加するが、このアドレスが改ざんされる恐れなどがある。しかし、たとえハッカーがアドレスの改ざんを図ろうとも、すべてのユーザーには自動的に元のアドレスを新しいアドレスの両方が通知される。以前はこういった機能を持つプラットフォームが存在しなかった。そしてこれはセキュリティ産業のパラダイムさえも転換させることができる。これまでは、多くの個人ユーザーに対し同時に攻撃を通知し、更なるダメージの拡大を防ぐ体系的な方法は存在しなかった。

未知の脅威予防(ユーザー側のシナリオ)

ハッカーのMalloyは有名な仮想通貨のオンラインコミュニティにソフトウェアをアップロードする。彼はこのソフトウェアを評判の高い脅威検出ウェブサイトであるVirusTotalやウイルス対策プログラムなどから検出されないようにした。Aliceを含む多くのコミュニティユーザーはこれを一見マイニングのソフトウェアだと思いダウンロードする。(残念ながらほとんどのユーザーはmd5やshaなどを通じて元のファイルの整合性を検査する術を知らない)。Malloyが彼のマイニングソフトウェア(バックドア)がダウンロードされたことを確認するや否や、彼はそれを通常のファイルへと置き換える。この時点で、最初にマイニングソフトウェア(バックドア)をダウンロードしたユーザーは既に侵されていて、すべての情報(ウォレットのプライベートキーのパスフレーズや取引所の個人情報)はMalloyによって集められている。しかしながら、どのようにしてシステムが侵されたのかを確認するのは難しい。一般のユーザーであるAliceはこのサイバー犯罪を捜査するために必要なスキルやツールを持ち合わせていないからである。

一方で、同じオンラインコミュニティユーザーの一人であるBobはSentinel Protocolのセキュリティウォレットを利用している。BobもAlice同様、感染したマイニングソフトウェアのダウンロードを行った。しかしながら、S-Walletの機械学習エンジンはファイルが非常に疑わしいことを検出する。このエンジンは、ウイルス対策ソフトに既知の攻撃であるとラベルや検出がされていなくても、このファイルの実行をブロックする。ファイルの実行がブロックされるとすぐに該当する情報が自動的にSentinel Protocolに提出される。その後、信頼されたセキュリティの専門家であるSentinelsがこの脅威の根本的な原因を解析する。こうして解析された情報は、脅威評価データベース(TRDB)に登録され、更にこのファイルが元々発見されたオンラインコミュニティにも報告される。タイムスタンプとアップローダーのより詳細な分析により、ここでMalloyはハッカーであると特定されてしまう。他方で、Malloyはすべての場所でSentinel Protocolデータベースのリアルタイム防衛システムが利用されていることから、彼のマイニングソフトウェアがどこにも配布できなくなっていることに気付く。

トランザクションの追跡可能性(ユーザー側のシナリオ)

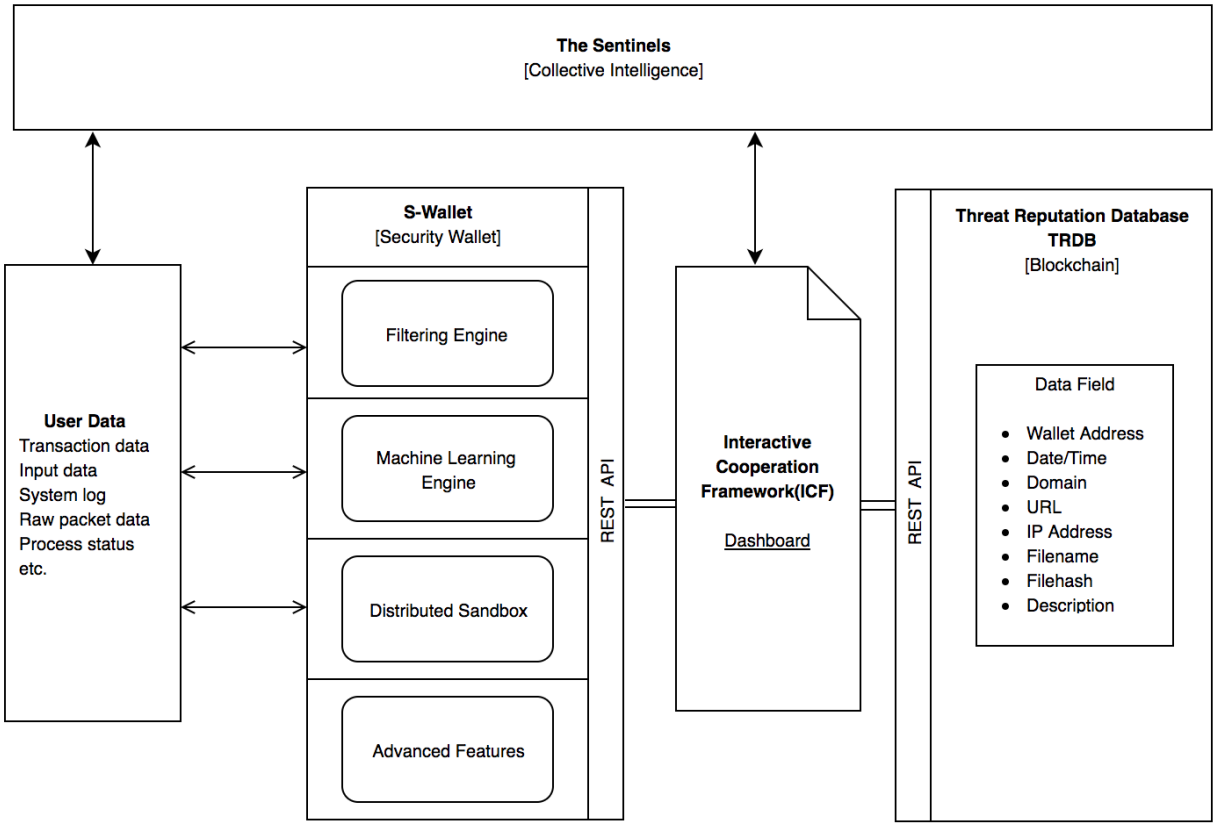
ハッカーのMalloyは多くの人々からハッキングによって奪ったコインを集めたウォレットを持っている。これを現金化する前に、彼は追跡を免れるためにコインを複数のサブアドレスに分散させる。仮想通貨のウォレットの性質上これは可能である。AliceはMalloyのハッキングの被害者である。彼女は自分のコインが盗まれていることを発見すると同時に、これをSentinel Protocolに報告する。すると、信頼されたセキュリティ専門家であるSentinelsが事件を確認しこの情報を脅威評価データベース(TRDB)に登録する。Sentinel Protocolはこの登録された元のアドレスから、すべてのサブアドレスを自動的に追跡する。この情報は、Sentinel Protocolを統合している、取引所を含むすべての仮想通貨サービスへと共有される。たとえMalloyが法定通貨への交換を試みたとしても、取引所は既に高い優先度の警告を受け取っているのでMalloyは奪ったコインを使うことができない。しかし、彼女がヨーロッパに住んでいてアメリカの取引所を使っていたケースを想定すると国境をまたいだ既存の司法システムのために奪われたコインを取り返すことは決して簡単なことではない。AliceはSentinel Protocolが世界中で広く存在感を持つことを望んで、この事件とSentinel Protocolを利用する優位性の積極的なプロモーションを始めた。いつか、ハッキングの報告のためにインターポールによって必要とされる法的な身分証明や複雑な文書の役割を、Sentinel Protocolが取って代わるほど影響力のあるものになるだろう。

チャプター9

システム設計

Sentinel Protocolは統合型セキュリティウォレットを通じてすべてのセキュリティサービスを提供する。しかしながら、それぞれの部分がAPIを利用したサードパーティとの連携を可能にするデザインとなっている。基本的には、統合型セキュリティウォレットは自動報告と手動報告の二つの機能が実装されている。

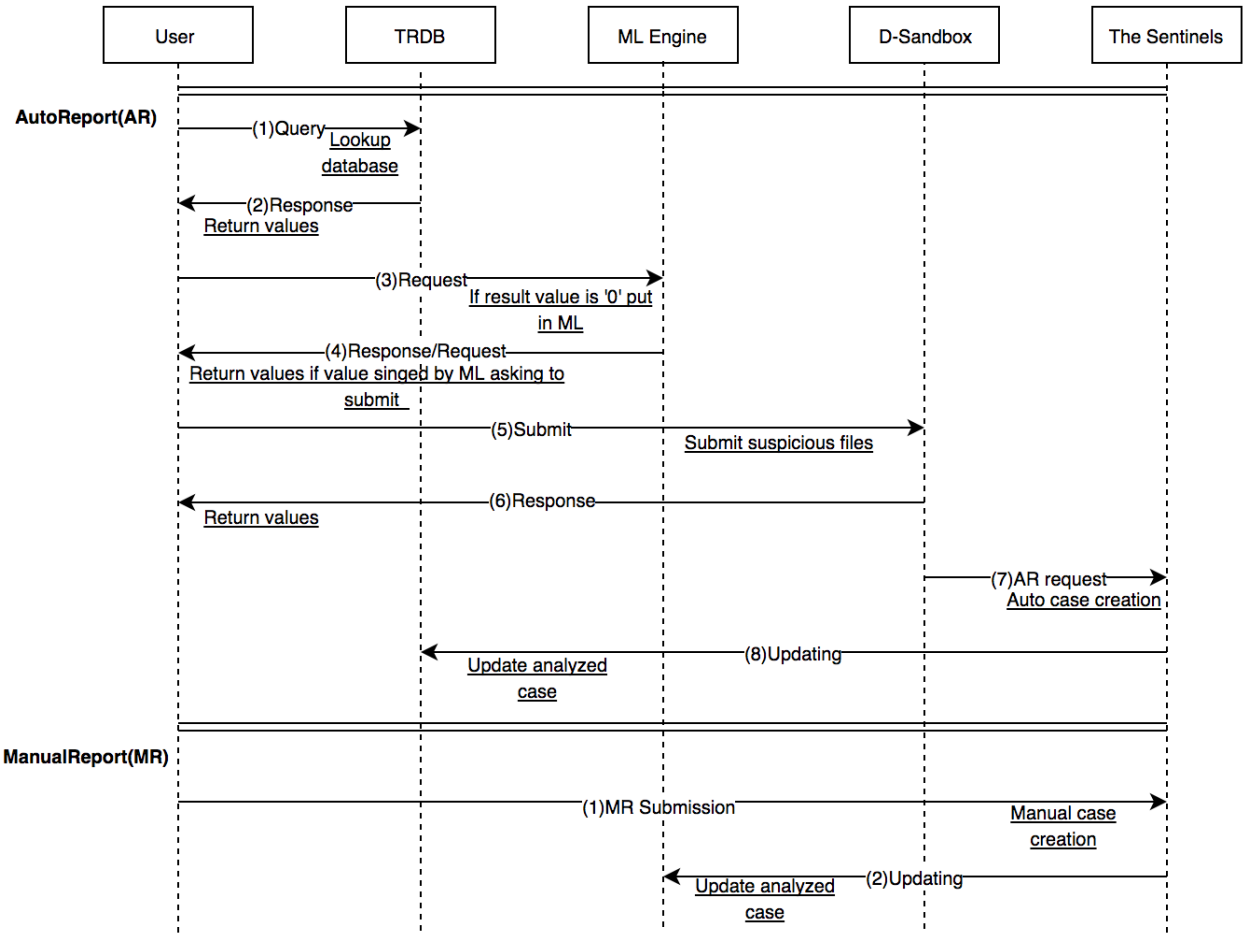
[技術的設計：Security Intelligent Platform for Blockchain(SIPB)]



- S-Wallet：統合型セキュリティウォレット
- User Data：ユーザーインプット、トランザクションデータ、システムログ、パケットデータ
- Filtering Engine：仮想通貨アドレスのフィルタリング、詐欺に関係するドメイン、URL、IP、ファイルのフィルタリング
- Machine learning Engine：挙動分析のためのローカル機械学習エンジン
- Distributed Sandbox：分散型マルウェア分析サンドボックス
- Threat Reputation DB：サイバー犯罪の情報を持つ知的データベース
- Plugin Features：将来的にVPNや統合型の第三ウォレットなどのセキュリティを向上させた機能を追加予定

- The Sentinels：認定資格を持つ集団的知性のグループもしくは個人
- Interactive Cooperation and Framework(ICF)：Sentinel Protocolとも呼ばれる。根本原因解析、インシデントレスポンス、世界中の活動の統計など、Sentinelsと個人ユーザーによって行われる活動のダッシュボードとなる。

[Security Intelligence Platform for Blockchain(SIPB)における処理のフロー]



ドメイン、URL、仮想通貨のウォレットアドレス、ファイルダウンロードなどがセキュリティウォレット実行中にリンクもしくはリダイレクトの形で実行された場合、以下の流れで処理が行われる。

自動報告(Auto Report)
自動報告は未知の脅威に対しての分析を最適化する知的フレームワークである。

1. Query：脅威データベースに報告された情報の潜在的な詐欺性・有害性の解析の問い合わせを行う。
2. Response：脅威データベースは登録された情報のデータフィールドを提供する。
3. Request：クエリされたアドレスが詐欺・有害と特定された際、単純にブロックを行う。特定されたものが新しいものでなかった場合も、ファイルがダウンロードされていれば、その解析を行うため機械学習エンジンに問い合わせを行う
4. Response/request：機械学習エンジンはファイルやプロセスの疑わしい挙動を解析し、未知の脅威としてブロックし、ユーザーにこの情報を報告するかどうかを尋ねる。

5. Submit：ユーザーがSubmitのオプションを有効にしていれば(On/Off選択可)、情報は分散型サンドボックスへと送信される。
6. AR Request：自動報告のケースとしてこの情報がICFのダッシュボードへと共有される。
7. Analysis Response：Sentinel達によってサンドボックスやそのほかのツールを利用した未知の脅威の解析が行われる。
8. Updating：更新された脅威の情報が脅威データベースへと送信される。

手動報告(Manual Report)

またユーザーは詐欺の情報を手動で報告することもできる。

1. MR Submission：疑わしい情報に関するドメイン、URL、詐欺アドレス、ファイルなどすべてをSentinel達に直接報告することができる。
2. Updating：情報が詐欺であると認められれば、更新された情報が脅威データベースへと送信される。

チャプター10

合意形成

Proof of Work(PoW)の基本的なメカニズムは、ブロック生成の権利を与え、マイニングを通じて目標とする難易度に到達した結果に対応した利益を支払うことである。この結果を見つけ出す作業は試行錯誤を重ねる莫大な計算能力を要するため、一部を除いてはこれを達成することは非常に難しい。したがって、これらの難しいプロセスを行ってきた者が大勢の代表者となることができる。しかし、この代表を探すためのプロセスにおける莫大な電力の無駄は一つの問題である。結果として、人々は合意形成を改善するための様々な方法にたどり着いた。代わりにProof of Stakeという理想的なアルゴリズムが創り上げられ、これはStakeの枚数によって代表になる確率が上昇するというものである。しかしながらこれらの二つのアルゴリズムは51%攻撃の問題を100%解決したわけではない。なぜなら、大勢の代表者の善意と悪意を区別することができないからである。

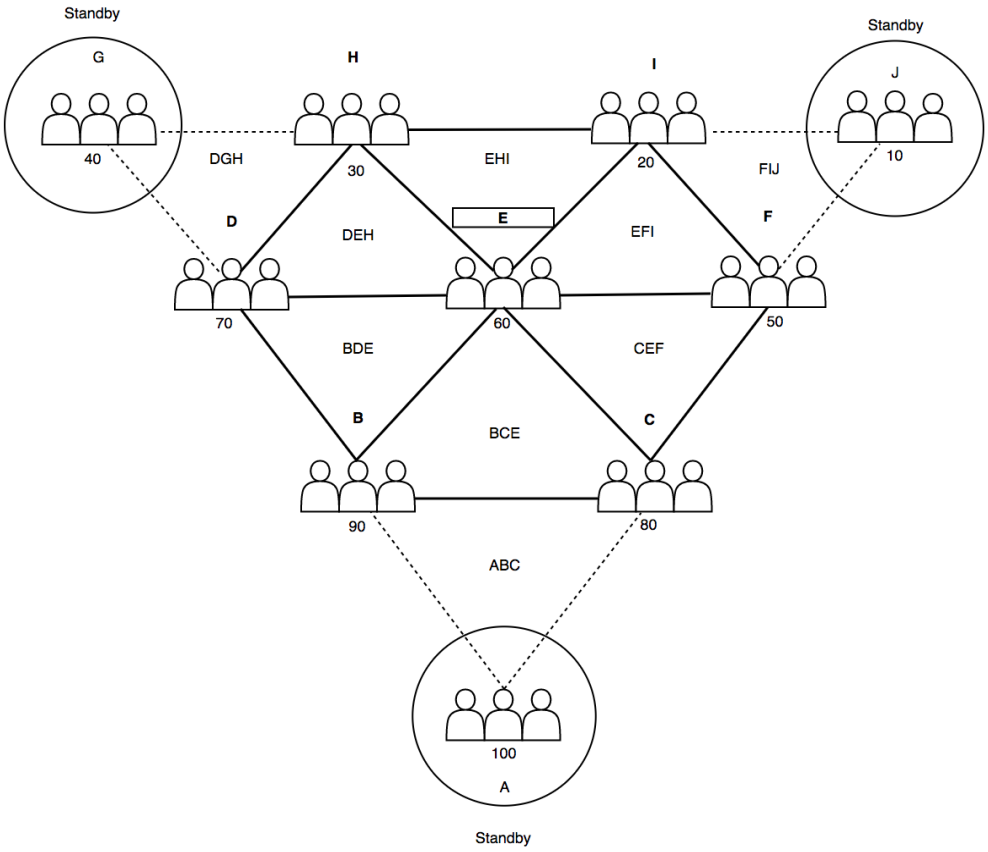
Sentinel Protocolの合意形成においてはBitshareによって導入されDaniel Larimerによって発案されたDelegated Proof of Stake(DPoS)というアルゴリズムが採用されている。Uppsala財団によって選抜されたSentinelは、仮想通貨取引所のセキュリティチーム、グローバルサイバーセキュリティ研究会社、或いはグループまたは個人のホワイトハッカーなど、必要最低限の資格を持つ、証明された機関や個人のグループで構成される。また、彼らの地位や経験はすべて証明されているものである。したがって、現実的に、リスクは劇的に軽減され、合意形成は最適化される。しかしながら、ソーシャルエンジニアリング的な視点とアルゴリズムの間にある溝は上述の通り否定できないものである。この問題を解決するために、評価のスコアはSentinel Point(SP)という、流通通貨であるUPとは別の配当として支払われる。Sentinel PointはSentinelのメンバーとして活動することによってのみ獲得することができる。例えば、APとMPで登録されたケースを解析し、脅威データベース内に関連する情報を記録、そしてそのデータに基づいて多くの産業は手助けを受けることができる。他の手段としては、彼らのパフォーマンスに基づいて、人々が実際に投票することもできる。評価スコアを獲得することで代表になるシステムはProof of Protection(PoP)と定義される。万が一、シビル攻撃やチェーンのフォークなど、Sentinel Protocolの誠実でないアクションが害を意図していたならば、罰としてSentinel Point(SP)を失うことになる。イーサリアムの事件と同様に、これはNothing at Stake（何も賭けていない状況）を消し去ることができ、代表者は評価と資格の両方を失う状況に常に晒されている。

この評価システム、特にこの構造にある優位性は、個人それぞれが、専門的な分野での信頼のもとに代表になっていることからも、悪人になることがほとんど不可能であるという点だ。正確には、この構造において、数多くのSentinelは合意形成を確実にするためのランダム性を向上させ、同時に不必要な遅延を生み出すだけの不必要な存在なのだ。したがって、Sentinel Protocolの合意形成の構造は、トランザクションの承認、ブロックの生成、脅威データベースの更新などを担当する７人のSentinelのみによって構成される小さなグループしか持たない。評価のランキングに応じて、合計10人のSentinelが選抜され、内７人はアクティブ状態、3人はスタンバイ状態となる。ネットワークのレイテンシーや遅延を取り除くために必要とされない限りは、この3人はスタンバイ状態を維持する。PoPの同期アルゴリズムと非同期ビザンチン障害耐性(BFT)(*10)は、大部分のSentinel同士がコミュニケーション取れなくなるほどの、重大なネット

ワーク断片化、大規模なDDoS攻撃、或いは、その他の予期しない出来事が起きた際の合意形成の予備アルゴリズムとしてサポートされている。

Sentinel ProtocolのProof of Protection(PoP)は、レイテンシー、スケーラビリティ、信頼性の観点からシンプルかつ効率的にデザインされている。

[高次の合意形成ダイアグラム]



- 代表する10の評価の高いSentinelが上述のような逆ピラミッド型の構造を組み立てる。
- ダイアグラム中の人々のグループそれぞれがSentinelを代表する(個人もしくは機関的に)。
- グループの下部に表示されている数字はコミュニティ貢献によって獲得したSentinel Point(SP)を表す。
- 端に該当するA,G,Jの３人はスタンバイ状態になる。
- 六角形のノードの中からランダムにブロック生成権が与えられる。
- 小さな三角形の構造は、効率を上げるためにブロードキャストの最小化のために最小単位のマルチキャストグループをタグ付けする意図がある。
- 7つの固定ノードによる最小化された合意形成プロセス
- ‘ｎ=3f+1’の構造に対してBFTが実装された場合、スタンバイ状態の３ノードによって最大10ノードまで操作することができる。またEがマスターになる。
- DoS(Denial of Service)耐性と高い利用可能性を備えたスタンバイノード、A,G,Jはピアノードのバックアップとして機能する。（安定した合意形成のために、Sentinelは強力なネットワーク環境を創り上げるが、DDoSなどの攻撃から100%守ることはできない。）

チャプター11

インセンティブシステム

Sentinel Protocolのねらいは、集権的なガイダンスや組織なしに適度のタイムフレームで自律的に維持ができるサイバーセキュリティのエコシステムを創造することである。効果的なサイバーセキュリティのエコシステムは、商品やサービスの用途を補うための直接的な方法として交換可能な仮想通貨を必要とする。また、それはサイバーセキュリティのエコシステムを改善するために個人の主観的な貢献を象徴する独立的な価値も必要とする。したがって、Sentinel Protocolは、Security Intelligence Platform for Blockchain(SIPB)によって供給される商品やサービスの利用のために流通させる仮想通貨をUPP(Uppsala)とし、Sentinel Protocolの評価に関しての価値を表すための通貨をSP(Sentinel Point)と名付けた。

初期段階で貢献したユーザーにはより多くのインセンティブが付与される。Sentinel Protocolが一定レベルの知性やタイムフレームに到達すると、初期段階での貢献者に利益を与えるために、比較的に類似する貢献に対してのUPP報酬の付与は自動的に削減される。このインセンティブのシステムは、サイバーセキュリティの専門家からの助けを必要とするユーザー、またこれに参加する専門家(個人か組織のどちらか)の両者を奨励するようにデザインされている。

[UPP (Uppsala)トークン]

- UPPはSIPBによって提供されるセキュリティウォレットのより進化した機能などの商品やサービスのための通貨である。
- UPPはまた、詳細なサイバーフォレンジックサービス、コンサルタント、脆弱性の評価、その他Sentinel Protocolのヘルプを必要とするケースでも使用される。
- 利用手数料は、Kyber Networkなどの分散型取引所(DEX)プラットフォームによってスマートコントラクトという形で徴収される。
- 最初に500,000,000UPPトークンが生成され、これは初期段階でサイバーセキュリティのコミュニティ形成に携わったユーザーに分配される。
- 20回に渡り、追加のUPPトークンが生成される。以下に説明されるインフレーション比率に応じて、Proof of ProtectionによってSentinel Protocolのよりよい環境を築いた貢献者に配布される。
- 初期段階の参加者やSentinelにインセンティブを付与するために、初期のインフレーション比率は3-7%に定められる。その後、各対数減分率は(おおよそ)0%のインフレーション比率に達するまで減少し続ける。
- 高度な機能の利用手数料、ケース処理手数料、財団による将来的な発展により得られたUPPトークンの30%もまた、コミュニティ貢献者への報酬としてUPPのインフレーションと共に付与される。
- 生み出されたSentinel Point(SP)が数週間のタイムフレーム、もしくはある一定の価値に達すると、コミュニティメンバーへの付与の権利が確定される。詳細なスキームは公式に発表される。
- 初期UPPの15%はUppsala財団のリザーブとして扱われる。
- 初期UPPの15%は、事業開発、開発資金、法的資金、顧問インセンティブ、その他の資金を必要とする組織的活動などに利用される。

- 初期UPPの２％は、顧問インセンティブのリザーブとして扱われる。
- 初期UPPの8%は、今後の予期せぬ事業活動のリザーブとして扱われる。
- 残りのUPP(初期UPPの60%)は、Sentinel Protocolの初期段階での貢献者、ユーザー、貢献者、サポーターなどのために市場に流通される。
- 初期UPPの交換比率は公式ホームページで確認することができる。

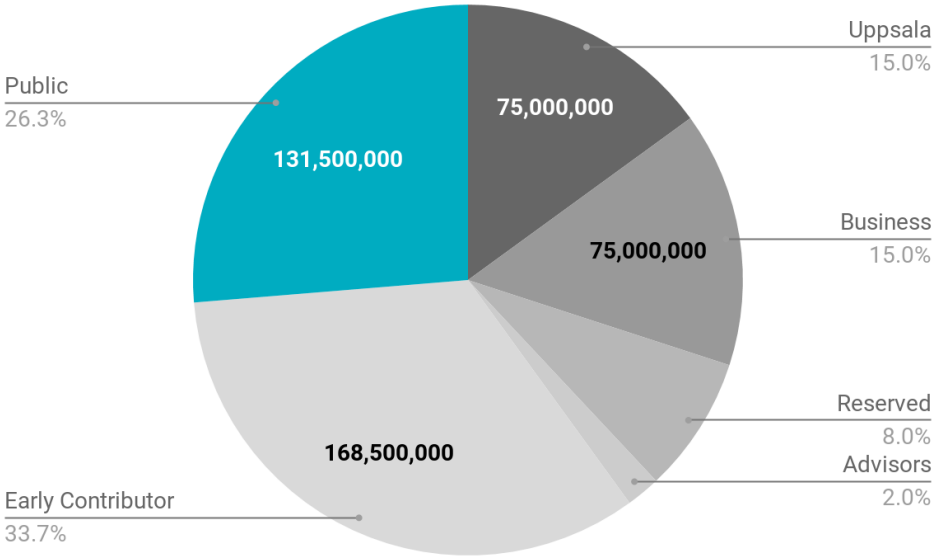
[Sentinel Point]

- PoP(Proof of Protection)によってのみ獲得可能。
- Proof of Protectionは、真の詐欺師のアドレス、IP、ウェブサイト、報告書の検証、事件の解決などの様々なサイバーセキュリティ活動によって成り立つ。
- 正当な報告の検証はSentinelによってのみ行われる。
- S-Walletを保有するユーザーは分散型マルウェア分析サンドボックスの計算を行うことでPoPを行うことができる。
- Sentinel Protocolコミュニティのための他の非直接的な貢献は、サイバーセキュリティの問題に関して大衆を啓蒙する内容の記事を書くことや、記事を他の言語に翻訳することなどを含む。
- The Sentinelsは報告の解析やユーザーによる評価の投票に応じてSentinel Pointを取得する。
- Sentinel Pointの保有者は、上述のUPPの生成において利益を得る。この際の利益額は、コミュニティのために行われたProof of Protectionを通じて生成されたSentinel Pointの総計に関連して、それぞれの集合が保有するSentinel Pointの割合を元に定められる。自動化された交換プロセスを適用することもできる。

[初期UPP分配スキーム]

Rounds	Number of UPP	Remark
Uppsala Foundation	75,000,000 (15% of Initial UPP)	-
Business Development	75,000,000 (15% of Initial UPP)	-
Reserved Allocation	40,000,000 (8% of Initial UPP)	-
Advisors	10,000,000 (2% of Initial UPP)	-
Early Contributor	168,500,000 (33.7% of Initial UPP)	-
Public Contributor	131,500,000 (26.3% of Initial UPP)	April ~ May 2018

[初期UPPの割り当て]



[調達資金の用途]

	資金の使途
研究・開発	50%
サイバーセキュリティへの設備投資	10%
営業・マーケティング	20%
運営・管理費	10%
会計・法務・コンプライアンス	10%

解説:

- 研究・開発: ロードマップに示されたとおりにプロダクトを開発するために利用
- サイバーセキュリティへの設備投資: 最新のサイバーセキュリティ技術を取り入れ、セキュリティチームを維持するために利用
- 営業・マーケティング: Sentinel Protocolのブランドの認知度を世界規模で成長させるためのオンライン・オフラインのマーケティングへの利用
- 運営・管理費: 日々のビジネス運営の出費
- 会計・法務・コンプライアンス: ビジネス運営における高い基準や透明性を維持するために利用

チャプター12

ロードマップ

Uppsala財団の設立と同時に、以下の活動が行われる。

Phase 1 – Sentinel Protocol of The Cryptocurrency World

18 Jan	HQ R&D center open in Singapore, APAC
	HQ R&D center security researchers integrate cybercrime, scam information existing in history, indexing into blockchain scheme Threat Reputation Database (TRDB)
	Regional R&D center developing Interactive Cooperation Framework (ICF) interface
18 Feb	SIPB prototype beta test
18 Mar	SIPB testnet launch with token issuance

Phase 2 – Proof of Protection

18 Jun	Public SIPB best release : The Sentinel Protocols serviced by sentinel protocol collective portal
18 Jul	Mainnet launch (The manual report of TRDB feature enabled into mainnet)

Phase 3 – Self Purification

18 Nov	Machine learning engine beta test
18 Dec	Machine learning engine feature release (auto report applied) beta
	Distributed sandbox (D-sandbox) release

Phase 4 – Self Evolution

2019	Machine learning based Fraud Detection System (FDS) release into mainnet

チャプター13

結論

Sentinel Protocolは既存のサイバーセキュリティのエコシステム、特に対策に本質的に欠けている、仮想通貨のセキュリティ産業において最も効率的なプラットフォームである。新たなベクトルの攻撃への先制的な対応においては、機械学習を利用したアプローチが最も効率的であると証明されている。しかしながら、可能性のみに基づく脅威の不明確さは依然として課題である。ブロックチェーンの集団的知性を用いたSentinel ProtocolのSecurity Intelligence Platform for Blockchainは仮想通貨のセキュリティ問題を解決するための、最も効果的かつ合理的なソリューションである。更に、高い参入障壁があると感じられている仮想通貨のセキュリティ産業は、間もなく多くのセキュリティベンダーが参入する手段となる。それによって、取引所、決済、ウォレットの企業などの仮想通貨産業と同時に存在する法的なシステムにより現在、保護されていないない多くの人々にとって、このコンバージェンスの肯定的な効果は偉大なものとなるだろう。Sentinel Protocolは適切なスキルを持つ個人が、ブロックチェーンの分散型セキュリティのための、この新しいプラットフォームに参加する機会を提供する。

参考文献

[1] SANS Institute InfoSec Reading Room /IT Security Spending Trends
: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697
[2] Cyber security market report: https://cybersecurityventures.com/cybersecurity-market-report/
[3] Hard Fork Completed: https://blog.ethereum.org/2016/07/20/hard-fork-completed/
[4] bitcoin: https://bitcoin.org/bitcoin.pdf
[5] Rep on the block: A next generation reputation system based on the blockchain
: http://ieeexplore.ieee.org/document/7412073/
[6] BlockSci Traces Transactions Performed With Dash, ZCash, and Other Currencies
https://themerkle.com/blocksci-succesfully-traces-transactions-performed-with-dash-zcash-and-other-currencies/
[7] A behavioural-based approach to ransomware detection
:https://labs.mwrinfosecurity.com/assets/resourceFiles/mwri-behavioural-ransomware-detection-2017-04-5.pdf
[8] Bitshares: https://bitshares.org/technology/delegated-proof-of-stake-consensus/
[9] Proof of Stake FAQ: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ
[10] Practical Byzantine Fault Tolerance: http://pmg.csail.mit.edu/papers/osdi99.pdf