IMES DISCUSSION PAPER SERIES

ブロックチェーン特有のネットワーク・セキュリティ：攻撃手法などの最新動向

面（おもて） 和成（かずまさ）

Discussion Paper No. 2022-J-2

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2022-J-2
2022 年 2 月

ブロックチェーン特有のネットワーク・セキュリティ：攻撃手法などの最新動向

面（おもて） 和成（かずまさ）*

要　　旨

ブロックチェーンの耐改ざん性および高可用性の性質を悪用したサイバー攻撃が観測されている。本稿では、ブロックチェーンのセキュリティのなかでも、ネットワークに関連する側面に焦点を当て、(1)ブロックチェーンへの攻撃、(2)ブロックチェーンを悪用した攻撃、および(3)ブロックチェーンに内在するセキュリティ・リスクについて最新の動向を報告する。(1)ではブロックチェーンを汚染するポイズニング攻撃や暗号資産を窃取しようとする攻撃を、(2)ではボットネットや暗号資産を騙し取るインフラをブロックチェーン上に構築する攻撃と、攻撃を観測するハニーポットの仕組みなどを、(3)では終了困難性や分散性低下といったブロックチェーン特有のセキュリティ・リスクを解説する。

キーワード：ブロックチェーン、スマート・コントラクト、暗号資産、ポイズニング攻撃、コマンド・アンド・コントロール（C&C）サーバ、ハニーポット

JEL classification：E42、O33、O36

* 筑波大学システム情報系（E-mail: omote@risk.tsukuba.ac.jp）

本稿は、日本銀行からの委託研究論文である。本稿の作成に当たっては、吉岡克成准教授（横浜国立大学）および大塚玲教授（情報セキュリティ大学院大学）から有益なコメントを頂戴した。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行や筑波大学の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

目　次

１．はじめに

近年、情報通信技術の発展に伴い情報システムの新しいプラットフォームとしてブロックチェーンの普及が進んでいる。ブロックチェーンは 2008 年にサトシ・ナカモトによって提案されたホワイト・ペーパー（Nakamoto [2009]）の中で、ビットコイン（Bitcoin）などの暗号資産の基盤技術として開発された。当初、ブロックチェーンはトランザクション（取引データ）を介した暗号資産の取引内容を保存しておくことを目的とした分散型台帳技術として用いられていた。

その後、ブロックチェーンにはスマート・コントラクトが導入され、ブロックチェーン上で動くさまざまなアプリケーションや情報システムの開発が可能となった。スマート・コントラクトではブロックチェーンの分散性やコンセンサス・アルゴリズムを応用し、信頼されていないユーザ同士が信頼できる第三者機関を介することなく互いにデータをやりとりしたり、トランザクションを送信したりすることが可能である。ブロックチェーンを用いた分散アプリケーションは DApps（Decentralized Applications）と呼ばれ、中央管理者を必要としない運営が可能となっている。また、ブロックチェーンはその特性を活かし、今では金融のみならず医療や IoT（Internet-of-Things）機器などのさまざまな分野においてその基盤を担っている。このようなスマート・コントラクトをサポートしている暗号資産プラットフォームとして最も有名なものにイーサリアム（Ethereum）が挙げられる。

しかし、暗号資産は財産的価値を有するため、サイバー攻撃の標的となるケースが増加している。例えば、Ethereum ネットワークを対象とした攻撃として、攻撃者が暗号資産を盗むために、Ethereum クライアントの脆弱なユーザ設定を悪用していることが確認されている。Ethereum のクライアントの多くは、デフォルトで 8545/TCP（Transmission Control Protocol）をエンドポイントとして設定するようになっている。このエンドポイントをインターネット上からアクセス可能な状態で運用する場合、送信元 IP（Internet Protocol）アドレスをフィルタリングするなどの必要があり、この重要性は、2015 年 8 月 29 日に Ethereum の公式ブログ（Steiner [2015]）にて述べられている。さらに、NICTER（Network Incident analysis Center for Tactical Emergency Response）観測レポート 2020[1]では、8545/TCP のポート番号に対するパケット数が近年増加していることを示しており、Ethereum が攻撃対象として選ばれていることを意味している。

本稿では、ブロックチェーンのセキュリティのなかでも、ネットワークに関連する側面に焦点を当て、ブロックチェーンへの攻撃、ブロックチェーンを悪用した攻撃、およびブロックチェーンに内在するセキュリティ・リスクについて最新

[1] https://www.nict.go.jp/cyber/report.html

の動向を報告する。ブロックチェーンへの攻撃では、特に影響が大きいブロックチェーン・データのポイズニング攻撃とブロックチェーンのアカウントへのサイバー攻撃について述べる。また、ブロックチェーンを悪用した攻撃では、ブロックチェーンをコマンド・アンド・コントロール（C&C）インフラの一部として使用する攻撃と暗号資産を騙し取るスマート・コントラクト・ハニーポットについて述べる。最後に、ブロックチェーンに内在するセキュリティ・リスクでは、ブロックチェーン・サービスにおける終了困難性とブロックチェーン・ネットワークの分散性低下のリスクについて述べる。なお、本稿におけるブロックチェーンはパブリック・ブロックチェーンを指す。

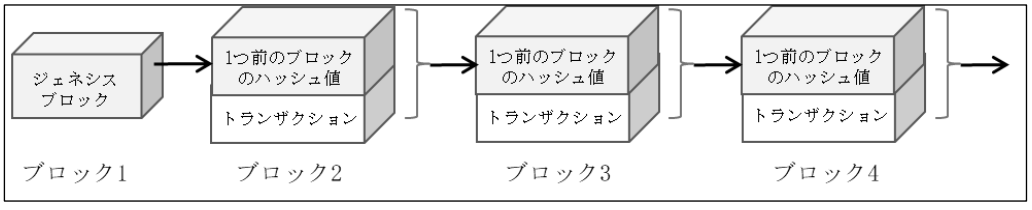
２．ブロックチェーンとネットワーク・セキュリティ

本節では、まずブロックチェーンと暗号資産について紹介したあと、ネットワーク・セキュリティに関して、ボットネット、ハニーポット、ダークネットについて説明する。

（１）ブロックチェーン

ブロックチェーンは、暗号技術的な側面とネットワーク技術的な側面の両面を併せ持つ技術であり、信頼できる第三者機関は必要なく、非中央集権的な P2P（Peer to Peer）ネットワークで価値を取引するためのセキュアな分散台帳を実現する。つまり、ブロックチェーンは、ブロックチェーン・ネットワーク上のノード間で共有されているトランザクションの台帳ともいえる。この台帳は、追加のみが可能なデータベースであり、変更や改ざんができない。図 1 にブロックチェーンのデータ構造を示す。各ブロックが 1 つ前のブロックのハッシュ値を含んでいるため、より前のブロックであるほどトランザクションの改ざんが困難となる。

図１　ブロックチェーンの基本的なデータ構造



ブロックチェーンのセキュリティの主な性質としては以下がある。

イ．耐改ざん性（暗号技術的な側面）

トランザクションがブロックチェーンに記録されると、それを改ざんすることは極めて困難である。その理由は、トランザクションの改ざんに伴ってそのブロックが変更されると、後続のブロックのハッシュ値がすべて変更されるため、あるブロックの改ざんを成功させるにはそれ以降のすべてのブロックを作り直さなければならないからである。そのため、後続のブロックが追加されるほど、そのブロックの耐改ざん性が増す。この性質は暗号技術で実現されている。

ロ．高可用性（ネットワーク技術的な側面）

ブロックチェーン・データが複数のノードによって多重化されているため高い可用性を有する。ブロックチェーン・ネットワークは、複数のノードによって支えられている P2P ネットワークであり、一時的なノードの故障、時折発生する一部の計算ノードの利用不能、ネットワーク遅延やパケット消失などに耐えるように設計されている。

（２）暗号資産

イ．Bitcoin

Bitcoin は、いかなる国にも限定されないグローバルな資産を目指す非中央集権的な暗号資産で最も有名なものである（Nakamoto [2009]）。Bitcoin はパブリック・ブロックチェーンを用いており、ブロックチェーンのセキュリティ性質である耐改ざん性と高可用性を有する。Bitcoin ネットワークは、中央サーバが存在しない P2P ネットワークであり、ノードが自由にネットワークに参加（離脱）できて、それでもなおシステムが機能する。また、非同期でもシステムが機能し、ネットワーク遅延やパケット消失が発生したとしても耐改ざん性と高可用性を有するため、システムは非常に堅牢である。さらに Bitcoin ネットワークは、システム的な単一障害点がないだけでなく管理主体もない、非中央集権的なネットワークであるといえる。Park *et al.* [2019] では、フル・ノード[2]と軽量ノード[3]のそれぞれのネットワーク・ノード数の計測を試みており、2018 年 1 月において観測期間 1 日でフル・ノードが 8,000 台、全ノードが約 50 万台を観測し、また 35 日間の観測ではフル・ノードが約 2 万台、全ノードが約 100 万台を観測している。

次に Bitcoin の送金の仕組みについて説明する。図 2 は Bitcoin の送金の概念図を示している。ここでは、A さんが B さんに 1BTC（BTC は Bitcoin の単位）

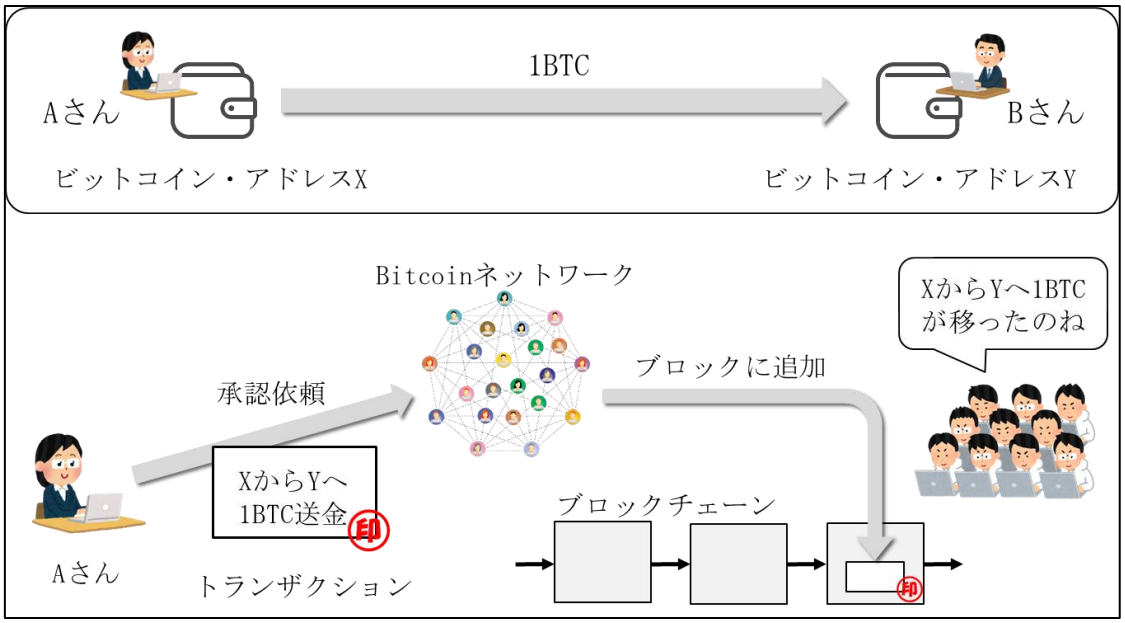
---

2 ブロックチェーンを持つノード。

3 ブロックチェーンを持たないノードであり、ブロック・ヘッダのみを持つ。SPV（Simplified Payment Verification）クライアントとも呼ばれる。

を送金することを考える。このとき、 A さんのウォレット[4]（Bitcoin アドレス X）から B さんのウォレット（Bitcoin アドレス Y）に 1BTC が送金される。なお、ここでは、便宜的に送金という用語を用いるが、何か電子的なお金が送られるわけではなく、暗号資産の価値の移転を指す。送金手順としては、まず A さんが「X から Y へ 1BTC 送金」というトランザクションを A さんのデジタル署名付きで Bitcoin ネットワークにブロードキャストして承認依頼を行う。承認がなされると、そのトランザクションがマイナーと呼ばれるノードによってブロックに追加され、そのブロックがブロードキャストされる。各参加者はその受け取ったブロックを検証し、問題なければそのブロックをブロックチェーンに追加する。ブロックチェーンは誰もがその内容を確認できるので、参加者はこの記録を参照することで X から Y へ 1BTC 移ったことに合意する。

図 2　Bitcoin の送金の概念図



Bitcoin のフル・ノードになるためには、ブロックチェーン・ネットワークに参加するためのクライアント（Bitcoin Core〈ビットコイン・コア〉）が必要となる。このクライアントがノードとなり、他のノードと接続されることによって、ブロックチェーン・ネットワークに参加することができる。また、クライアントを介して、トランザクションの発行などのさまざまな操作を行うことが可能となっている。さらに、Bitcoin Core は JSON-RPC（JavaScript Object Notation-Remote

4 財布を意味する言葉であるが、暗号資産が直接入っているわけではなく、鍵（公開鍵／秘密鍵）に関するデータが収められている。

Procedure Call）を利用して遠隔操作が可能となっている。JSON-RPC とは、HTTP（Hypertext Transfer Protocol）プロトコルの POST メソッドであり、JSON 形式のリクエストを送信することにより遠隔からプログラムに処理を依頼するためのプロトコルである。Bitcoin Core では、JSON-RPC の Basic 認証[5]を設定でき、デフォルト設定ではローカルからのみパスワードでアクセスできることに注意する。

ロ. Ethereum

Ethereum とは、パブリック・ブロックチェーンをベースとした分散アプリケーションのための分散型プラットフォームである（Buterin [2013]）。Ethereum 内には、Bitcoin と同様に暗号資産が実装されており、イーサ（Ether）と呼ばれる。また、Ethereum には、スマート・コントラクトと呼ばれるプログラムを実行する仕組みが導入されている（Ethereum Virtual Machine（EVM）については後述）。Ether は、スマート・コントラクトを実行するための手数料の役割も担っている。Ethereum には、Externally Owned Account（EOA）と Contract Account（CA）という 2 種類のアカウントが存在する。EOA はユーザのアカウントであり、ユーザの秘密鍵によって管理される。EOA と紐付く秘密鍵を持つユーザは、その EOA から Ether を送ったりコントラクトの生成や実行をしたりすることができる。一方で、CA はスマート・コントラクトが持つアカウントである。Ethereum におけるスマート・コントラクトについては本節（4）を参照されたい。

Ethereum を使用するためには、Bitcoin と同様に、ブロックチェーン・ネットワークに参加するためのクライアントが必要となる。Go Ethereum（Geth）[6]や Parity Ethereum[7]などの複数のクライアントが存在している。さらに、これらのクライアントは、Bitcoin 同様に JSON-RPC を利用して遠隔操作が可能となっている。これにより、ユーザが Ethereum ノードに対して送金などのトランザクションの発行や Ethereum ネットワークの状況の確認、マイニングなどのさまざまな操作を遠隔から行うことができる。しかしながら、Ethereum のクライアントは Bitcoin と異なり、JSON-RPC の Basic 認証を設定できない。デフォルトでは JSON-RPC は有効化されていないが、Ethereum には web3.js[8]やスマート・コントラクトがあるため、クライアントを外部から JSON-RPC 経由で利用することが多いと考えられる。エンドポイントに対してファイアウォールなどのアクセス制御を

---

[5] Bitcoin では、RPC を待ち受けるアドレスはデフォルトで外部に公開しない設定（localhost）となっている。外部に公開する場合は簡易的な認証（Basic 認証）しか用意されていない。

[6] https://geth.ethereum.org/

[7] https://www.parity.io/technologies/ethereum/

[8] Ethereum で利用可能な JavaScript ライブラリ。

かけておらず、外部の攻撃者からアクセスされた際には、ノードの操作権限を攻撃者に奪われる可能性がある。Ethereum クライアントにおいて JSON-RPC の機能を有効にするには、セキュリティ面に十分に注意する必要がある。

Ethereum のウォレットとして有名なものに METAMASK[9]がある。METAMASK は、GoogleChrome、Firefox、Opera などの主要ブラウザの拡張機能として実装された Ethereum のウォレットであり、プライベート・ネットワークへの接続や ERC20 （Ethereum Request for Comments 20）準拠のトークンの送信にも対応している。

ハ．アルトコイン

アルトコインとは Alternative Coin の略称であり、Bitcoin 以外の暗号資産のことを指すことが多く、さまざまな機能や運用理念を持っている。知名度の高いアルトコインとしては、Ethereum、ライトコイン（Litecoin）、ドージコイン（Dogecoin）などが挙げられる。アルトコインは Bitcoin 同様にブロックチェーンが用いられることが多く、暗号資産における価格追跡ウェブサイト CoinMarketCap[10]がモニタリング対象としているものだけでも、2021 年 7 月の段階で 2,500 種類以上が存在している。

（３）暗号資産ブロックチェーンへの非金融データの埋込み

ブロックチェーンは、暗号資産の送金に関する金融データだけでなく非金融データを埋め込むことができる領域が存在する。この領域を利用することで、文書の存在証明やログなどのフォレンジック[11]が可能となる。ここでは、主流な暗号資産である Bitcoin と Ethereum における非金融データの埋込みについて述べる。

イ．Bitcoin

Bitcoin は暗号資産に特化しており、スマート・コントラクトの実行などは想定していないものの、任意のデータを埋め込むことができる公式の領域が存在する。Bitcoin において意図して設計されたデータの埋込み可能な領域は、スクリプトの一命令である OP_RETURN による 80 バイトの領域と、マイナーのみが自由なデータを書き込むことができる Coinbase による 96 バイトの領域である。しかし、Coinbase はマイナーしか書き込めないため、一般の参加者は OP_RETURN を用いて最大 80 バイトのデータを埋め込むことができる。

---

9 https://metamask.io

10 https://coinmarketcap.com/all/views/all/

11 法的証拠を見つけるための鑑識調査。

ロ. Ethereum

Ethereum は、スマート・コントラクトなど非金融データを埋め込むことが想定されている暗号資産であり、init/data 領域と extraData 領域の大きく 2 種類の領域が存在する。init/data 領域はスマート・コントラクトの生成・利用に使用される領域である。仕様上の上限は存在しないが、トランザクションの手数料はブロックごとに決められた手数料（gasLimit）を超えることができないため、実質の上限（数百キロバイト）は存在している。さらに Go Ethereum（v1.6.6）では、32 キロバイト以上のデータを init/data 領域にもつトランザクションはトランザクションプールに入る段階で拒否する処理が追加されている。一方、extraData 領域は Ethereum ブロック・ヘッダに存在する領域であり、マイナーのみが書き込める領域である。この領域は 1 つのブロックにつき 32 バイトしかないため、ファイルを埋め込むためには十分でない。したがって、一般の参加者は init/data 領域にデータを埋め込むことになる。

（4）スマート・コントラクト

スマート・コントラクトとは、ブロックチェーン上で契約を自動的に実行する仕組みのことである。これは自動販売機によく例えられ、利用者が硬貨を投入し、ボタンを押すと契約が成立するのに似ている。実際には、トランザクションを発行することによって、コントラクト（プログラム）がブロックチェーン上に配置されたり、コントラクトが実行されたりする。コントラクトはブロックチェーンを持つすべてのノードが実行する。

Ethereum におけるスマート・コントラクトは、Ethereum ネットワーク上の Ethereum Virtual Machine（EVM）と呼ばれる仮想マシンが EVM コードと呼ばれるバイトコードを実行することによって実現される。Solidity[12]などで記述されたコントラクトはコンパイラによって EVM コードにコンパイルされる。そして、ユーザがトランザクション（Contract Creation Transaction）にその EVM コードを格納して送信することによってブロックチェーン上に CA が作られる。このコントラクトを実行するためには、生成された CA に対してユーザがコントラクトの引数をもったトランザクションを送信することが必要となる。そのため、Ethereum のトランザクションには EVM コードを Ethereum ネットワークに送信するための init という領域と、スマート・コントラクトの実行時に引数を渡すためなどに使用される data という領域が存在する。これらの領域は、プログラムのバイトコードやプログラムへの引数を載せるという性質上、書き込まれる内

[12] https://github.com/ethereum/solidity

容とサイズの両面から非常に自由度の高い領域である。

（５）ブロックチェーン・エクスプローラ

Bitcoin や Ethereum のような主流な暗号資産では、ブロックに格納されている情報を取得できるウェブサイトが第三者によって運営されている。これはブロックチェーン・エクスプローラと呼ばれており、特殊なソフトウェアや CLI（Command Line Interface）などを用いることなくブラウザからブロックやトランザクションの内容を確認することができる。そのため、ブロックチェーンを持たない者（軽量ノードや一般ユーザ）にとって非常に便利なものである。ただし、表示される情報の正確性はウェブサイトの信頼性に依存しており、フィルタリングによって一部の内容が表示されない可能性もあることに注意が必要である。具体的なブロックチェーン・エクスプローラとしては、Bitcoin における BLOCKCHAIN[13]や Ethereum における Etherscan[14]がよく知られている。ブロック・ハッシュ、トランザクション・ハッシュなども参照可能であり、特に Ethereum では init/data 領域のデータや、コントラクトのソース・コードなども公開されている。

（６）メインネットとテストネット

不特定多数のノードが参加できるパブリックなブロックチェーンである Bitcoin や Ethereum には、メインネットとテストネットの 2 種類が存在している。ここでは、Ethereum を例にとって説明する。メインネットは、本番環境のネットワークであり、ここでは市場価値のある Ether が送金されたり実運用されているスマート・コントラクトが稼働したりしている。一方でテストネットとは、主に開発者がテストのために使用する Ethereum ブロックチェーンであり、メインネットとほぼ同様の仕組みを持つ。これにより、メインネットのように送金などを行うことが可能である一方、テストネット内で使われる Ether に市場価値は無い。Ethereum では、メインネットとテストネットはデフォルトで同じポート番号 8545/TCP が使用されているため、攻撃者は調査を行うまでは対象のノードがどちらのネットワークに所属しているかを判断できない。

（７）ボットネット（Botnet）と C&C サーバ

Botnet のボット（Bot）とは、マルウェアなどに感染したコンピュータのことであり、管理者の知らないところで悪意ある命令が実行される。Bot は外部のサーバ（コマンド・アンド・コントロール：C&C サーバ）から制御されるとい

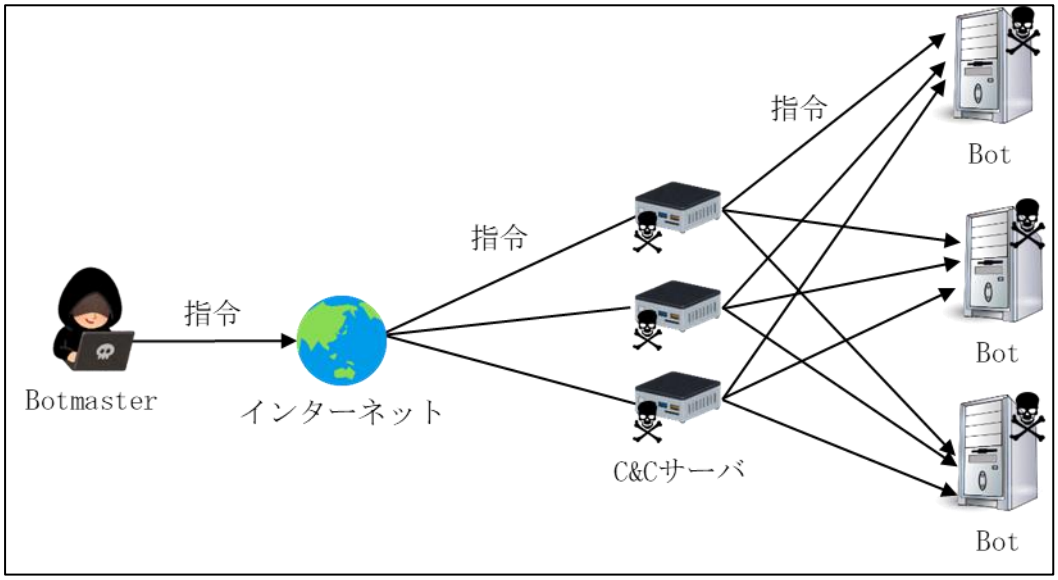
---

13 https:// www.blockchain.com/ja/explorer

14 https://etherscan.io

う特徴を持つため、Botnet は外部から制御可能なネットワーク（Bot 群）であるといえる。図 3 は、C&C サーバ型ボットネット（Botnet）の全体図を表している。Botnet の管理者であるボットマスター（Botmaster）はすべての Bot を管理する必要はなく、中間的な管理サーバである C&C サーバに対して指令を出すだけでよい。C&C サーバは Botmaster から受け取った指令を Bot に伝達してくれる。実際には、Botmaster がこの C&C インフラを使って数十万台の Bot を制御するといったことが行われており、指令を受けた Botnet が DDoS（Distributed Denial of Service）攻撃やスパム・メール送信など悪意ある活動を行う。さらに、Botnet の規模を維持・拡大するために、各 Bot が感染拡大活動も行う。

図 3　C&C サーバ型 Botnet



（８）ハニーポット

ハニーポットとは、攻撃されることを意図したコンピュータのことである。故意に攻撃させることにより、攻撃者がどのような操作をし、どのようなツールを使用し、どのように攻撃するのかを知ることができるため、防御側が主導権を握ることができる。ハニーポットへの通信には正当なトラフィックは存在せず、収集したほとんどのデータに価値がある。しかしながら、攻撃者にハニーポットと気づかれた場合、ハニーポット端末が乗っ取られたり、検知を避けるために偽の情報を与えられたりするリスクが存在する。そのため、ハニーポットと気づかれないようにする工夫が必要である。なお、後述の 4 節（2）のスマート・コントラクト・ハニーポットは、ここで説明する一般的なハニーポットと異なることに注意する。

（９）ダークネット

ダークネットとは、インターネット上で到達可能である未使用 IP アドレス空間のことを指す[15]。未使用 IP アドレス空間に対してパケットが送信されることは、通常のインターネットの利用ではほとんど起こりえないものであるが、SHODAN[16]やマルウェアなどによる端末の探索行為によって、パケットがダークネットに到達することがありうる。したがって、ダークネットに到達するパケットを観測すれば、インターネット上での端末の探索行為など不正な活動の傾向把握が可能になる。

３．ブロックチェーンへの攻撃

暗号資産・ブロックチェーンへの攻撃としては、ネットワークの計算能力の過半を独占して不正な取引を強引にブロックチェーンに埋め込むことなどを可能とする 51%攻撃や、すでに使用した暗号資産をもう一度使用する二重支払い攻撃などが有名である。Li *et al.* [2020] では、このようなブロックチェーンのリスクを分類しているが、本節では比較的新しい攻撃であるブロックチェーン・ポイズニング攻撃、およびブロックチェーンへのサイバー攻撃について紹介する。

（１）ブロックチェーン・ポイズニング攻撃

イ．概要

ブロックチェーンに違法なデータや悪質なデータを埋め込むことによりブロックチェーン自体が違法・悪質なものとなってしまう可能性がある。これをブロックチェーン・ポイズニング攻撃と呼ぶ。一般的な公開データベースに対するポイズニング攻撃として広く知られているものとして、DNS（Domain Name System）キャッシュ・ポイズニング[17]がある。この場合、攻撃内容の検知ができれば、悪意あるデータの削除や修正が可能である。これに対し、ブロックチェーンへのポイズニング攻撃の場合、ブロックチェーンのデータの取消しや修正が極めて困難であるという特性から同様の対応ができない。また、ブロックチェーンに埋め込まれた情報は P2P ネットワークを通じて世界中のフル・ノードに拡散される。

ブロックチェーン・ポイズニング攻撃は、攻撃の目的によって、イミテーション攻撃、DoS（Denial of Service）攻撃、プライバシー攻撃に分類することができる（木村・今村・面［2021］）。イミテーション攻撃はデジタル・アート作品の贋

---

15 https://www.nict.go.jp/publication/NICT-News/1205/page/NICT_1205_9p.pdf

16 インターネット上でアクセス可能な機器の情報を収集・公開しているウェブ・サービス。情報収集には端末の大規模な探索が行われている。

17 IP アドレスとドメイン名を対応付ける DNS のキャッシュ情報を意図的に書き換える攻撃。

作をブロックチェーンに埋め込んで、それをブロックチェーン上で売却することによって不正に利益を得ることを目的とする。この攻撃では、デジタル・アート作品の贋作が不正に流通されるだけでなく後で取消しが不可能となる。DoS 攻撃はマルウェアやアダルト画像など所持が違法となる可能性がある悪性データをブロックチェーンに格納することでブロックチェーン・サービスを妨害することを目的とする。この攻撃では、所持が違法となるデータがブロックチェーンに格納されると所持を避けるためにフル・ノードの離脱が誘発され、ネットワークの可用性が低下してしまうおそれがある。プライバシー攻撃は個人を特定するようなデータをブロックチェーンに格納することで個人情報を暴露することを目的とする。この攻撃では、個人のプライバシーを侵害するだけでなく、取消しが不可能となる情報が埋め込まれる。いずれのポイズニング攻撃も、ブロックチェーンに任意のデータを埋め込める領域が存在するために可能となる攻撃である。また、世界中のフル・ノードが攻撃の影響を受けることに注意されたい。

ブロックチェーン・ポイズニング攻撃のおおまかな流れは次のとおりである。①悪意あるユーザがトランザクションを用いて悪性データをブロックチェーンに送信する。②マイニングにより悪性データがブロックに格納される。③悪性データを格納したブロックが P2P によりネットワーク全体に伝搬する。④ネットワーク全体が悪性データによって汚染された状態になる。

ロ. Bitcoin に対するポイズニング攻撃

Matzutt *et al.* [2018a, b] では、Bitcoin のブロックチェーンに対するデータの埋込みについて調査している。具体的には、Bitcoin のブロックチェーンに任意のデータを埋め込むことの利点と危険性について議論し、実際に Bitcoin ブロックチェーンに対して埋め込まれたデータについて調査した。その結果として、児童ポルノへのリンク集など多くの国で違法な可能性の高いファイルやプライバシーを侵害する内容を含んだファイルが Bitcoin のブロックチェーンに埋め込まれていることが明らかになった。さらに、OP_RETURN を用いた公式の手法では最大 80 バイトのデータしか埋め込むことができなかったが、非公式な手法では 100 キロバイト程度のデータを埋め込むことができることを明らかにした。具体的には、通常のトランザクションであっても発行時点で検証できない値（公開鍵や一部ハッシュの値など）を任意のデータに差し替えることが可能である。また、マイナーによるチェックが不十分[18]であることを期待して、通常のトランザクション・テンプレートから逸脱した規格外のトランザクションを用いることも可能である。さらに、それらの手法を応用してユーザがブロックチェーンの構造

[18] チェックが不十分なマイナーの実在についても指摘されている。

やデータの埋込み手法を意識せずに、ブロックチェーンにデータを埋め込むことのできる「データ埋込みサービス」が存在することも示している。

ハ. Ethereum に対するポイズニング攻撃

Ethereum では、トランザクションに Bitcoin よりも大きなデータを埋め込む領域が用意されている。そのため、Bitcoin を用いる場合よりも攻撃の幅が広がると考えられる。多くの Ethereum ウォレットはトランザクションの init/data 領域に書き込むデータを 16 進数文字列の形で受け取り、それを送信することが可能となっている。したがって、この機能を用いることで任意のデータを Ethereum ブロックチェーン上に埋め込むことができるため、ファイルなども 16 進数の状態に変換することで埋め込むことが可能となる。

Sato, Imamura, and Omote [2019] では、Ethereum ブロックチェーンに対するデータの埋込みについて調査している。具体的には、ブロックに含まれるトランザクションの init/data 領域に書き込まれたデータに対して、ファイル・カービング[19]を用いて分析を行い、実際にどのようなファイルが埋め込まれているのかを調査した（最初のブロックからブロックの Height 6,803,255（2018 年 11 月 30 日）までの分析を行っている）。検知の対象としているファイルは、jpg、gif、png、bmp、avi、exe、mpg、wav、riff、wmv、mov、pdf、ole、doc、zip、rar、html、cpp の 18 種類である。その結果、153 個のファイルの埋込みが確認できている。

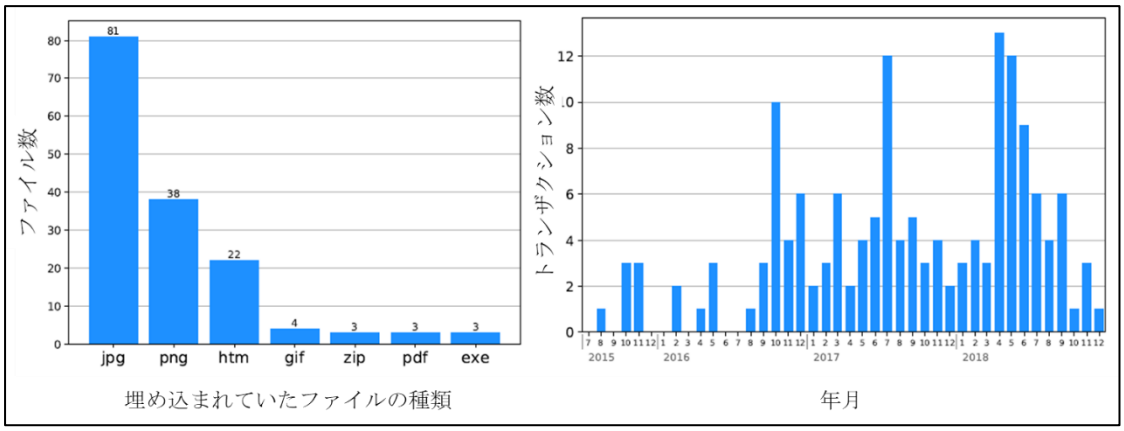
図 4 の左側のグラフは、調査範囲の Ethereum ブロックチェーンに埋め込まれたファイル内訳を示している。ファイルの種類に関しては、jpg と png の画像ファイルが大部分を占めている。画像ファイルの内容としては、集合写真や人物写真やイラストや模様などの画像であり、その内容に違法性がないと思われるファイルが大部分であったのに対し、好ましくない内容の画像ファイルも複数見つかっている。exe ファイルは 3 つのファイルが見つかっており、VirusTotal[20]で検索した結果、「W32.Duqu」などマルウェアであることを突き止めている。図 4 の右側のグラフは、ファイルの埋込みを検知したトランザクションについて、そのトランザクションの発生時期（2015 年 7 月 30 日～2018 年 11 月 30 日）の分布を示している。この結果より、ファイルが埋め込まれているトランザクションの数は 2018 年後半で減少しているものの、概ね増加傾向にあったことがわかる。

---

[19] ファイル・カービングとは、ファイルの種類ごとのシグネチャ情報を検索してファイルを探す手法である。

[20] VirusTotal は 70 種以上のアンチウイルス・ソフトを用いてファイルや IP アドレス、URL が悪性かどうかを判定するウェブサイトである（https://www.virustotal.com/gui/home/）。

図 4　Ethereum ブロックチェーンに埋め込まれたファイル内訳と埋め込まれた時期



資料：Sato, Imamura, and Omote [2019]

ニ．対策

Matzutt *et al.* [2018a] では、Bitcoin ブロックチェーンを対象として、好ましくないコンテンツの埋込みに対する 1 つの対策として、データ・サイズが大きいほどトランザクションの経済的コストを上げる手法が提案されている。Bitcoin ブロックチェーンは大量のコンテンツを格納する仕様にはなっていない。しかし、悪意あるユーザは意図されていない埋込み手法を用いて、サイズの大きい好ましくないコンテンツを埋め込むことができる。そこでこの研究では、悪意の有無に関わらずトランザクションを発行する参加者全員に埋め込むデータのサイズに比例した経済的ハードルを課すことを提案している。これにより、サイズの大きな好ましくないコンテンツの埋込みを減らす効果が期待される。しかし、埋め込まれるデータの悪質性はデータ・サイズに相関しないと考えられる。

Kiffer, Levin, and Mislove [2018] によれば、実際に利用されるコントラクトは使い回しなどによって類似しているものが多く存在していることが明らかになっている。この研究結果を用いて、Sato, Imamura, and Omote [2019] では、Ethereum ブロックチェーンを対象として、データ・サイズによらない新たな対策を示している。具体的には、マイナーがコントラクト・プールに保有する複数のコントラクトからそれぞれのコントラクトの類似度を計算し、その類似度が低いほどコントラクトを登録するための経済的コストを高くする。これにより、悪意あるユーザが非合法なデータもしくは違法性の高いコントラクトを利用する場合、他のコントラクトとの類似性が低いため、攻撃者にはコスト面で大きな負担がかかることになる。また正規のコントラクトは類似するものが多いため、比較的安いコストでコントラクトを作成できることが期待される。

これらの対策では、コンテンツのデータ・サイズやコントラクトの類似度に応

じた手数料がブロックチェーンのプロトコル上で設定されていることを前提とするため、ブロックチェーン・システムが攻撃者に対してコスト面で負担をかけることによって攻撃を緩和する対策となる。

（２）ブロックチェーンのアカウントへのサイバー攻撃

イ．概要

ブロックチェーンのアカウントは、オンライン・バンキングのアカウントと同様に資産を直接的に扱うことができる。アカウントへのサイバー攻撃がその窃取に直結するため、本攻撃は暗号資産を窃取することを目的として実行される。

ブロックチェーンは、P2P 型の分散ネットワークにより運用されるサービスであり、柔軟性と運用性の点からインターフェースに JSON-RPC という遠隔操作が実装されている。Bitcoin や Ethereum でも JSON-RPC によるリモート・アクセス機能が用意されている。これに関して、脆弱で管理されていないインターフェースに対して、遠隔操作を悪用した攻撃が報告されている。

NICTER 観測レポート 2020 では、8545/TCP のポート番号（Ethereum における JSON-RPC API のデフォルト・ポート）に対するパケット数が近年増加していることを示しており、攻撃対象としてランク外から 9 位にランクインしている。つまり、Ethereum における JSON-RPC エンドポイントに対する 8545/TCP のアクセス制御が適切になされていないものがあるという認識が拡がり、これらを狙った攻撃者が増加していると推察される。ここでは、活発化している Ethereum ネットワークを対象としたサイバー攻撃に焦点を当てる。

これまでの研究において、攻撃者が暗号資産を盗むために、Go Ethereum や Parity Ethereum などの Ethereum クライアントの脆弱なユーザ設定を悪用していることが確認されている。これらのクライアントは、アクセス制御およびパスワードが適切に設定されていないと、アカウントの保有者に代わって、攻撃者が Ethereum アカウントをリモートから操作することが可能になる。そして最悪のケースとして、EOA アカウントのロックが解除されてしまい、暗号資産が不正送金される危険性がある。このような攻撃の実態調査の研究がいくつかなされている。

ロ．Ethereum へのサイバー攻撃の観測

Cheng *et al.* [2019] では、ハニーポット（彼らが管理する Ethereum クライアント）を設置することによって、Ethereum クライアントの JSON-RPC のデフォルト・ポートへの攻撃を 6 ヵ月間観測している。具体的には、1,072 件の異なる IP アドレスから収集した 3 億 800 万件以上の RPC リクエストを分析し、全リクエストの 83.8%を占めている 9 つの IP アドレスが主な攻撃の発生源となっている

ことを明らかにしている。これにより、JSON-RPC API のデフォルト・ポートへの攻撃が実際に行われていることが確認された。加えて、一部の攻撃者が大量のリクエストを出していることも明らかにし、特に攻撃準備として、アドレスを取得する eth_accounts メソッド、および対象のアドレスが所持している Ether の残高を確認する eth_getBalance メソッドが大量に使用されていることも明らかにしている。さらに、ブロックチェーン・ネットワーク上には RPC ポートが何のアクセス制限もなく解放されている脆弱な Ethereum ノードが存在していることも示されており、攻撃対象となりうるノードは多く存在していることが指摘された。

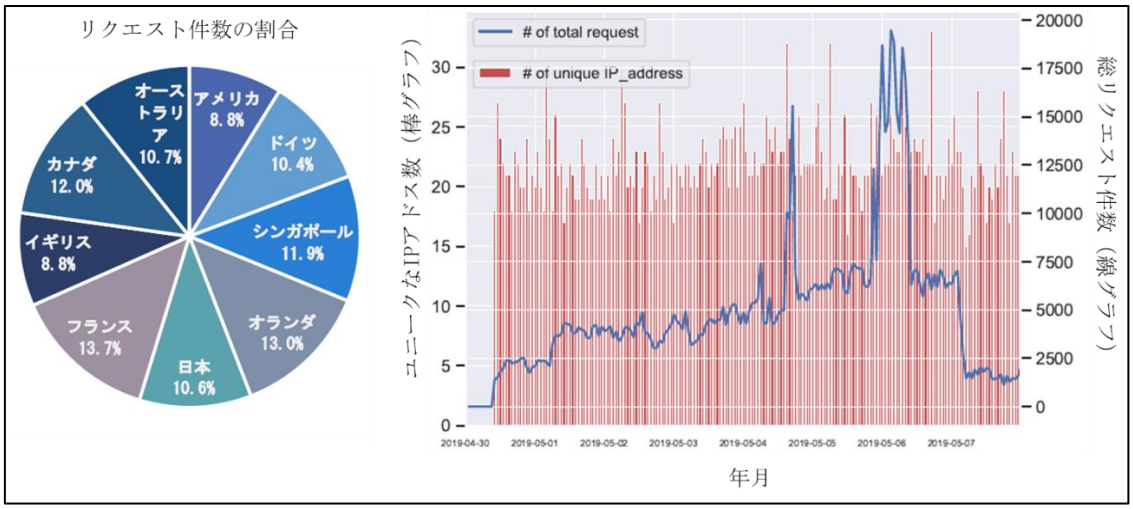
Hara *et al.* [2020] では、ハニーポット（彼らが管理する Ethereum クライアント）を世界各地に分散して設置することによって、Ethereum クライアントの JSON-RPC のデフォルト・ポートへの攻撃および攻撃者の特徴について、より詳細な分析を実施している。本研究では、次の 3 つの攻撃的通信の判定基準に着目し、メソッドの詳細な分析を行うことで、攻撃者が Ethereum ネットワークにて不正に利益を得ようとしていることを明らかにしている。

- ハニーポットへの送信： 攻撃者は、Ether の窃取を目的として、ハニーポットに対して RPC リクエストを送信する。本来、ハニーポットへの RPC リクエストは管理者しか行わない。
- ダークネットへの送信：攻撃者は、脆弱な Ethereum クライアントを探索するために大量の RPC リクエストをインターネットに向けて大規模かつ無作為に送信する。その結果、RPC リクエストがダークネットに到達してしまう。本来、RPC リクエストがダークネットに到達することはありえない。
- メインネットかどうかの調査 : 攻撃者は、実際に市場価値のある暗号資産が取引されているメインネットに対して接続を試みる。しかし、メインネットとテストネットはデフォルトで同じポート番号 8545/TCP を使用しているため、攻撃者は攻撃対象とする Ethereum クライアントがメインネットに存在するかどうかを事前に調査する。このとき、net_version メソッドなどを使用することによってメインネットかどうかを判定できる。本来、Ethereum クライアントがメインネットに存在するかどうかを調査する事由はない。

実験においては、ハニーポットを世界 9 ヵ国（オーストラリア、カナダ、ドイツ、フランス、日本、オランダ、シンガポール、イギリス、アメリカ）に設置し、総リクエスト件数は 956,151 件（観測期間は 2019 年 4 月 30 日から 2019 年 5 月 7 日までの 8 日間）であった。国別にリクエストの傾向を分析した結果、図 5 の左側の円グラフのとおり、まず国による偏りが見られないことを明らかにした。

さらに、1 時間ごとに発生しているリクエスト件数と、それらのリクエストの送信元のユニークな IP アドレスに対する分析を行い、図 5 の右側のとおり、同 IP アドレスが増加しているわけでもないのにリクエスト数が急増している時期があることから、サイバー攻撃が同時期に発生していたものと判断している。このほか、Ether の残高を確認する eth_getBalance メソッドが大半を占めることも明らかになった。さらに、①リソースを無駄にしないように攻撃対象をメインネットのみに絞る、②大規模かつ無作為にリクエストを送信している、といった 2 パターンの攻撃があることも明らかにしている。なお、攻撃者が net_version メソッド、または eth_getBlockByNumber メソッドを実行することで、対象ノードがメインネットで稼働しているノードか否かを確認している様子も観測している。

図 5　リクエスト件数の国別割合と各時刻における総リクエストの件数とユニークな IP の数



資料：Hara *et al.* [2020]

これら 2 つの研究（Cheng *et al.* [2019]，Hara *et al.* [2020]）により、「悪意あるユーザは eth_accounts メソッドでアドレスを取得し、そのアドレスを引数として eth_getBalance メソッドでアドレスの残高を取得する」という攻撃前の事前調査の基本シナリオが明らかになった。もし悪意あるすべてのユーザがこの基本シナリオに従うのであれば、ハニーポットにおいて残高があるかのように見せる「偽の残高」を返すことで、その後の詳細な攻撃を観測することが期待できる。しかし、悪意あるすべてのユーザがこの基本シナリオに従うとは限らない。一部の悪意あるユーザは、eth_getBalance メソッドに頼ることなくブロックチェーン・エクスプローラなどの外部サービスから真の残高を取得するかもしれない。したがって、「偽の残高」を返す方法では、残高がゼロであることが攻撃者に露見

されるため、その後の暗号資産を窃取しようとする攻撃を観測できない可能性が存在する。

陳・面［2021］では、効率的かつ効果的なハニーポットの設置に向けて上記の基本シナリオに関する詳細な分析を行っている。ここでは、次のようなハニーポット設置の要件を明らかにした。

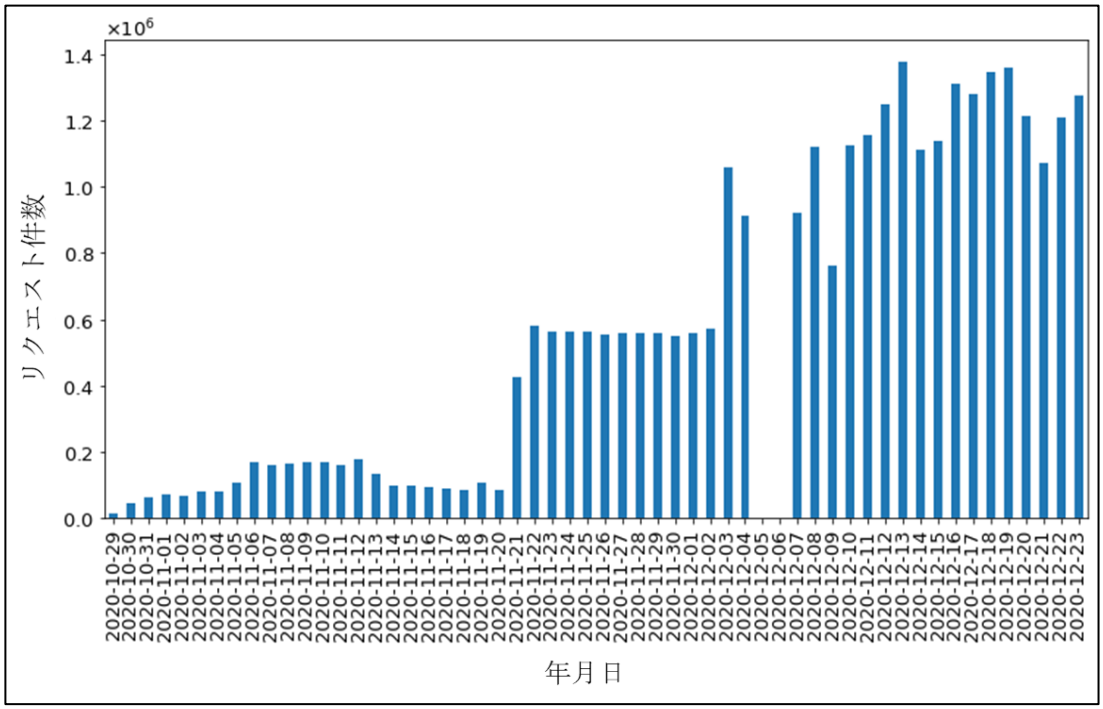
- ハニーポットは実際に暗号資産を保有する必要がある。悪意あるユーザに対して餌となる「ノードで管理されている暗号資産の残高」として、残高があるかのように見せる「偽の残高」を返す方法では、すべての攻撃を観測できない。
- ハニーポットは必ずしも実際に市場価値のある暗号資産が取引されているメインネットに参加する必要はなく、リクエストに対してメインネットに参加しているかのようなレスポンスを返せば十分である。この場合、メインネット参加に伴うサーバのストレージ容量などのコストを削減できる。

1 番目の条件については、ハニーポットのアドレスに本物の Ether を置くことで悪意あるユーザの挙動を実際に観測している。具体的には、2020 年 11 月 21 日にハニーポットのアドレスに 0.2ETH を置くが、そのアドレスの残高を取得する eth_getBalance メソッドに対しては「残高なし」を返すように設定した。つまり、悪意あるユーザはメソッドのみでは間違った情報を入手するように仕掛けられている。しかし、図 6 に示すとおり 2020 年 11 月 21 日に不正送金を試みようとする攻撃のリクエストが急増しており、攻撃対象のノード以外から残高に関する情報を取得していることが推測される。ただし、2 番目の条件にあるとおり、メインネットに参加しているか否かについてはレスポンスによって悪意あるユーザを騙すことができる。

また、王ほか［2021］も、Ethereum クライアントの JSON-RPC のデフォルト・ポートへの攻撃および攻撃者の特徴について分析しており、エクリプス（Eclipse）攻撃[21]など、これまでの研究では観測されていない攻撃を観測している。

[21] ターゲット・ノードを Ethereum ネットワークから隔離する攻撃手法。

図 6　リクエスト件数の推移



資料：陳・面［2021］

ハ．対策

Ethereum へのサイバー攻撃では、残高のあるアドレスを探し出し、RPC によるリモート・アクセスによってその暗号資産を窃取しようとする攻撃がメインである。Ethereum では、JSON-RPC に対してアクセス制御をかけられないが、暗号資産に紐付いているアカウントにはメソッドなどを利用するためのパスワードを設定できる。このパスワードが破られると、Ether の送金権限が奪取され不正送金が可能となるだけでなく、アカウントの秘密鍵も奪取される。そのため Ethereum へのサイバー攻撃対策では、Ethereum クライアントを管理する各参加者が自身のアカウントのパスワードを強固にすることが基本である。さらに、Hara *et al.* [2020] では、このエンドポイントをインターネット上からアクセス可能な状態で運用する場合、送信元 IP アドレスをフィルタリングするなどファイアウォールが必要であることを指摘している。つまり、Ethereum クライアントを管理する各参加者にとって、インターネットからアカウントに到達するまでに、Ethereum クライアントへのアクセス制御（ファイアウォールなど）、および Ethereum クライアント内にあるアカウントへのアクセス制御（パスワード）という二重のアクセス制御を設置することが重要である。

４．ブロックチェーンを悪用した攻撃

本章はブロックチェーンを悪用する攻撃について述べる。攻撃者は、耐改ざん性と高可用性を有する強固なブロックチェーン・インフラを利用できるメリットがある。実際に、こうした攻撃が出現しており、特に Ethereum を悪用する攻撃が発見されている。例えば、暗号資産のネットワークを悪用してサイバー攻撃実行のためのインフラを構築したり、スマート・コントラクトを悪用して暗号資産を窃取したりするものが存在する。ここでは、ブロックチェーンの C&C サーバ化、およびスマート・コントラクト・ハニーポットの新しい 2 つの話題について取り上げる。

（１）ブロックチェーンの C&C サーバ化

イ．ブロックチェーン上に C&C サーバを構築する理由

ブロックチェーンを用いない場合、一般に Botmaster は C&C サーバを自前で用意しなければならないだけでなく、多くの Botnet は C&C チャネル（C&C サーバと Bot を繋ぐネットワーク）が発見され乗っ取られることで破壊されるという弱点を有する。つまり、Botnet にとってはいかに C&C チャネルを秘匿し、破壊されにくくするかということが課題となる。

このような背景から、攻撃者には、耐改ざん性や高可用性を有するブロックチェーン・インフラを用いることにより、破壊されにくい強固な Botnet の C&C チャネルを構築できるというメリットが存在する。Botmaster はすでに構築されているブロックチェーン・インフラを C&C サーバとして利用できる。また、各 Bot はブロックチェーンからデータを取得すればよいため、Bot 間の通信が不要となる。Böck *et al.* [2019] では、ブロックチェーン上に C&C サーバを構築する理由として次の 5 つを挙げている。これらの理由により、Botmaster は多くのメリットを享受する。

- 匿名性：トランザクションを発行する Botmaster の匿名性（仮名性）をある程度実現できる。
- ロバスト性：ブロックチェーンの高可用性により C&C インフラを破壊できない。
- 数え上げ耐性：Bot が正規ユーザに紛れるため Bot の台数を数え上げることができない（Botnet の全体像が見えない）。
- ステルス性：C&C 通信がブロックチェーンの通信に紛れる。
- 単純性：Bot がブロックチェーンの P2P ネットワークに参加することが容易である。

ロ．ブロックチェーンを用いた C&C 攻撃

ブロックチェーンを用いた C&C 攻撃では、Bot が Botmaster からの攻撃命令などを入手する方法として、攻撃方法①：Bot 自身がブロックチェーン・ネットワークにノードとして参加する方法、および攻撃方法②：ブロックチェーン・エクスプローラを利用する方法の 2 通りが存在する（Sato, Imamura, and Omote [2019]、木村・面［2020］）。

攻撃方法①：Bot がフル・ノードになってローカルのブロックチェーンから情報を取得する方法である。Bot がブロックチェーン・ネットワークに参加しているケースであり、通常のノードと同様に P2P ネットワークを通じてローカルのブロック内から攻撃命令などを取得する。ブロックチェーンのデータがローカルに保存されているため、この手法は Bot が指令を受け取るために通信を発生させる必要がないという特徴がある。例えば、暗号資産のウォレット・アプリケーションが動作しているサーバ（フル・ノード）を標的としたマルウェアなどであれば、この手法を用いることでネットワーク通信による攻撃の検知が困難となる。

攻撃方法②：Bot がブロックチェーン・エクスプローラから情報を取得する方法である。ブロックチェーンの情報は公開情報であるため、ブロックチェーン・ネットワークに参加していなくても、Bot はブロックチェーン・エクスプローラを利用して、ブロック内に格納されている Botmaster からの攻撃指令やマルウェア・プログラムを得ることが可能である。この手法の特徴として、企業などのネットワークにおいても HTTP(S)の通信は許可されていることがほとんどであるほか、HTTPS の通信であれば取得している詳細な情報が暗号化されており攻撃であることが検知されにくいことなどが挙げられる。さらにこの手法の最大の利点は、悪意がないウェブサイトであるブロックチェーン・エクスプローラをマルウェアの通信先とすることにより、ウェブサイトを閲覧してブロックチェーンの情報を調べている通信とマルウェアによる通信の判別を困難にするという意味でステルス性を高めている点である。

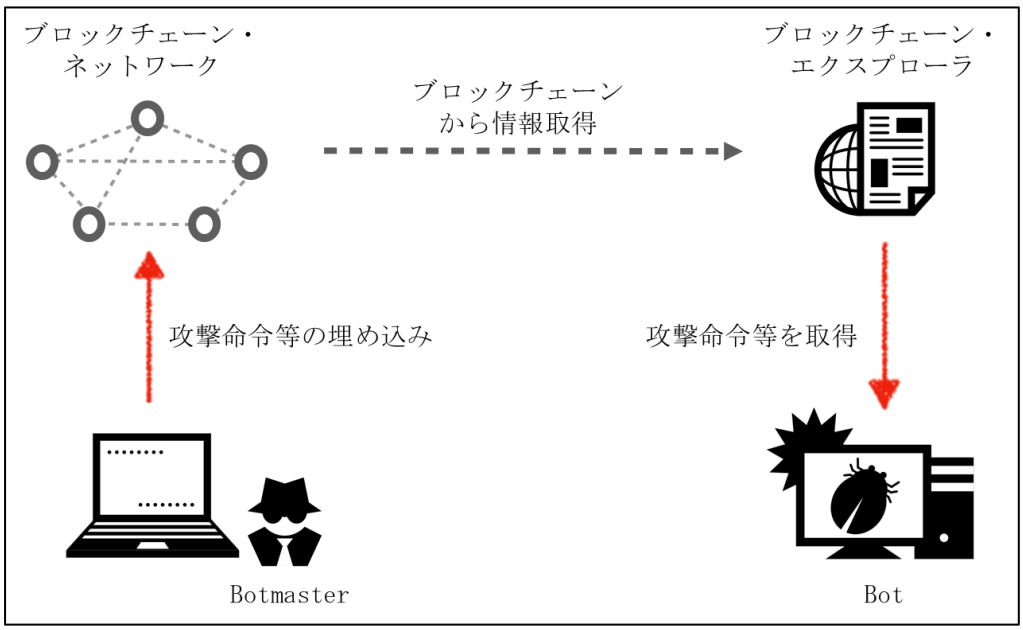
ここでは、攻撃がより容易である攻撃方法②について詳しく説明する。図 7 は攻撃方法②の具体的な流れを示している。

1. Botmaster は、ブロックチェーンの自由な領域に対して、Bot への指令やドロッパーにダウンロードさせるマルウェア自体をブロックチェーンに埋め込む。

2. ブロックチェーン・エクスプローラが、ブロックチェーンの情報を同期することによってブロックチェーンに埋め込まれた悪意ある情報（攻撃命令）を取得する。
3. Bot（すでに感染している端末など）はブロックチェーン・エクスプローラに接続して、新たな攻撃命令やマルウェアの更新プログラムなどを取得する。

ブロックチェーン・エクスプローラを用いることで、Bot はブロックチェーンを持つ必要がなくなる。さらには、ウェブ・アクセスが許されている世界中のすべての Bot に攻撃命令を届けられる点が脅威となる。攻撃命令はバイトコードとしてブロックチェーン内に記載され、それがウェブ・サービスで公開される。ブロックチェーン・エクスプローラではこのバイトコードが単なるウェブサイトの情報となるため、ウェブ・アクセスが許されている Bot は攻撃命令を容易に取得できる。このような特徴を利用することで、マルウェアの C&C 通信インフラやドロッパーと呼ばれるマルウェアのダウンロード元として、ブロックチェーンを悪用することが可能である。

図 7　ブロックチェーンを用いた C&C 攻撃（ブロックチェーン・エクスプローラを利用したケース）



資料：Sato, Imamura, and Omote [2019]

ハ．ブロックチェーンの C&C サーバ化における欠点

ブロックチェーンを利用したこれらの攻撃手法には共通した欠点が存在する。

それはブロックチェーンに埋め込んだ情報は取り消したり変更したりすることができない点である。例えば、マルウェアをブロックチェーンに埋め込んでいることが明らかになってしまえば、マルウェア自体の解析を逃れることができない。ただし、埋め込んだマルウェアなどがブロックチェーン・データの調査によって明らかになってしまうことを防ぐために、マルウェアを複数のトランザクションに分割したり、何らかのエンコード・暗号化を施したりすることで、発見を遅らせることは可能である。

ニ. Bitcoin ベースの C&C サーバ化

Ali *et al.* [2015, 2018] では、Bitcoin ネットワークを利用することによって、ブロックチェーンを C&C サーバ化して Botnet の C&C 通信を実現する手法（ZombieCoin）の実現可能性について議論している。この論文では、公式のデータ埋込み手法以外にも C&C の通信内容を Bitcoin のトランザクションに埋め込む方法があることを示している。さらに、Bitcoin ネットワークを C&C インフラの一部として利用することで破壊が困難となることや、インフラの維持のためのコストやリスクを回避できるなどの理由からこの手法が実現性と実用性を持っていることを主張している。また、検証のための Botnet を実際に構築し、Bitcoin のメインネットにおいて C&C 通信を行い、その評価も行っている。評価の中では、Bot がブロックチェーンの更新のタイミング（Bitcoin の場合は約 10 分間隔）でブロックチェーンを検索するのではなく、攻撃の情報を含むトランザクションがネットワーク全体に伝播するのに合わせて 5〜12 秒間隔でトランザクションを受信できることを示している。これは、攻撃にかかるすべてのトランザクションが最終的にマイナーによって拒否されたとしても、Bot はすでにそれらを受け取り、検証し、攻撃命令を実行できることを意味する。

Pletinckx, Trap, and Doerr [2018] では、Bitcoin のトランザクションに C&C サーバに接続するための情報を隠しておき、各ボットはそれを見て Tor ネットワーク[22]に隠れている C&C サーバに接続するという方法が提案されている。この手法の利点としては、ネットワーク上に不自然な痕跡が残らないという点が挙げられる。具体的には、トランザクションは一時的な Bitcoin アドレス（公開鍵の最初の 6 文字が C&C サーバのドメイン名を含むように細工する）に送付され、各 Bot は C&C サーバにアクセスするために抽出されたアドレスに接続するというスキームが紹介されている。

---

[22] The Onion Router の略。インターネット上に設けられた複数のノード（オニオン・ルータ）を経由させてカプセル化を行い、発信元の匿名性を高めて通信を行うシステム。

ホ. Ethereum ベースの C&C サーバ化

Ethereum は Bitcoin と比較して、格納できる任意のデータ量が多いため、より C&C サーバ化に利用しやすいと考えられる。例えば、Bitcoin の OP_RETURN を用いる場合、80 バイト以下の攻撃命令や不正プログラムを 1 つのトランザクションに埋め込むことができるが、80 バイトを超えるとそれらを複数のトランザクションに分割して埋め込む必要が出てくる。その結果、Botmaster や Bot にとって余計な処理が増えるデメリットが生まれる。これに対して、Ethereum では 1 つのトランザクションに数百キロバイトの攻撃命令や不正プログラムを格納できるため、Botmaster や Bot にとって利便性が高いといえる。

Sato, Imamura, and Omote [2019] では、Ethereum ネットワークを利用することによって、ブロックチェーンを C&C サーバ化して Botnet の C&C 通信を実現する手法の実現容易性について議論している。具体的には、実環境を模倣した検証環境を構築し、検証環境内のプライベート・チェーンに対してファイルの埋込みと取出しを行っている。この検証では、簡単なターミナル・コマンドとブラウザのみでファイルの埋込みと取出しが可能であることを示している。ブラウザは Google Chrome を使用し、METAMASK を Google Chrome にインストールして利用する。今回の検証実験ではファイルの hexdump を取得するためにターミナル・コマンドを使用している。ファイルの埋込みでは、ファイルを 16 進数文字列に変換した後、トランザクションを利用してブロックチェーンに埋め込む。ファイルの取出しでは、ブロックチェーン・エクスプローラのウェブサイトをブラウザで参照すれば埋め込まれた 16 進数データに容易にアクセスできる。表示された 16 進数文字列からはファイルを復元できる。

へ. 対策

Ali *et al.* [2015, 2018] では、Botmaster と思われるアドレスをブラックリスト化することで C&C 通信を防ぐというこれまで考えられてきたような対策方針に対して、プロトコルの大幅なアップグレードが必要であるため現実的ではないと言及している。さらに、暗号資産のアドレスは誰でも簡単にいくつでも作成することができ、かつ、アドレスが本人と直接結びつくものではないため、Botmaster にアドレスを次々に新規作成されればアドレスによるフィルタリングでは C&C 通信を防ぐことができないと指摘している。

木村・面［2020］では、前述の 2 つの攻撃シナリオに対するトランザクション単位のフィルタリング対策について、その基本手法と限界を示している。ブロックチェーンの中に含まれているデータの中で悪性データがどれであるかはセキュリティ・ベンダなどによって事前に把握されていると仮定する。この場合、悪性データが格納されたトランザクションに対してブラックリストを作成する

ことによって、トランザクション単位でフィルタリングが可能になる。ブロックチェーン参加者が上記のブラックリストを参照してフィルタリングを行うことを想定し、そのパフォーマンス検証を試みている。具体的には、シェル・スクリプトを用いて簡易的なフィルタリング機能を実装し、データベースを使用しないナイーブなケースとして、10 秒で約 1,500 件のブラックリストのフィルタリングが可能であることを示している。

（2）スマート・コントラクト・ハニーポット

イ．スマート・コントラクトの脆弱性を狙う攻撃

ブロックチェーンのアカウントには、ユーザのアカウントだけでなくスマート・コントラクトのアカウントも存在し、プログラムであるスマート・コントラクトが直接的に暗号資産を保有できる。こうしたスマート・コントラクトは参加者が自由に作成し、ブロックチェーン・ネットワーク上にデプロイ（展開配置）することができる。それゆえ、例えば Ethereum では、悪意あるユーザがバグのある脆弱なスマート・コントラクトを探して、資産を騙し取ろうとする攻撃が存在する。スマート・コントラクトが暗号資産を直接的に扱う性質を考えると、スマート・コントラクトの脆弱性は壊滅的な結果につながる可能性がある。スマート・コントラクトは、一度ブロックチェーンにデプロイされると基本的に不変であり、さらにそうしたコントラクト・コードにパッチを当てることは基本的に不可能である。

ロ．Ethereum におけるスマート・コントラクト・ハニーポット

Ethereum においてスマート・コントラクトのハニーポットが設置されていることが明らかになっている（Torres, Steichen, and State [2019]）。これは、スマート・コントラクトの脆弱性を狙う攻撃者をだます攻撃者の存在を表している。一般にハニーポットは攻撃を観測するために設置されることが多いが、このハニーポットは攻撃者から暗号資産を騙し取ることを目的とした新しいタイプのハニーポットである。具体的には、高スキルの攻撃者（攻撃者 A とする）が暗号資産を騙し取ることができるように見えるコントラクトを設置し、このコントラクトに餌となる暗号資産を入れておく。そして、このコントラクトを用いて、別の低スキルの攻撃者（攻撃者 B とする）から逆に暗号資産を騙し取ろうとする手口が知られている。これはスマート・コントラクト・ハニーポットと呼ばれ、欠陥を持つように「みえるように」意図的に設計されたコントラクトであり、その欠陥を悪用しようとする攻撃者 B を誘うものである。スマート・コントラクト・ハニーポットでは、欠陥を悪用しようとする攻撃者 B に対して一定量の Ether の送金を要求することが多い。つまり、一定量の Ether の送金を行えば、欠陥の

あるコントラクトを実行できるように設計されている。攻撃者 B は一定量の Ether を預けて、その何倍もの Ether を騙し取ろうとするが、結局は騙し取ることに失敗し（コントラクトが騙し取られないように設計されている）、逆に預けた Ether が奪われるというものである。攻撃者 A は、低スキルの攻撃者 B に対して欠陥（見せかけ）の検出を容易にするためにソース・コードをあえて公開する。

ハ．対策

Ethereum におけるスマート・コントラクトは一度ブロックチェーンにデプロイされると不変となり、コードの削除ができないだけでなく、バグにパッチを当てることもできないため、基本的には永続的に不正利用されるリスクが存在する。そのため、開発者にとってスマート・コントラクトの脆弱箇所をデプロイ前に特定できることが望ましい。スマート・コントラクトの脆弱性検出に関する研究はこれまでに数多く提案されている。例えば、DSL（Domain Specific Language）を用いた手法（Tsankov *et al*. [2018]）、シンボリック実行[23]による手法（Luu *et al.* [2016]）、トランザクションから検出する手法（Zhang *et al.* [2020]）、ソース・コードから検出する手法（芦澤ほか［2020］）などが存在する。

Ethereum におけるスマート・コントラクト・ハニーポットは、悪意あるユーザ（低スキルの攻撃者）を誘い込む不正なスマート・コントラクトであるため、善意のユーザにとってはリスクが低いと考えられる。しかし、これまで以上に巧妙な手口で善意のユーザを騙して暗号資産を窃取するような悪質なスマート・コントラクトが今後出現しないとも限らない。そのため、スマート・コントラクト・ハニーポットを含む不正なスマート・コントラクトを放置することは善意のユーザにとっても望ましいことではない。

スマート・コントラクト・ハニーポットに対する対策手法については、セキュリティ・ベンダなどがそのような不正コントラクトを検知することが考えられる。Torres, Steichen, and State [2019] はスマート・コントラクト・ハニーポットの検知手法を初めて提案している。これは、上記のスマート・コントラクト・ハニーポットの分析を世界で初めて実施した研究であり、同時にスマート・コントラクト・ハニーポットの分類法も提供している。さらに、スマート・コントラクト・ハニーポットを検出するために Solidity バイトコードに対してシンボリック実行を行うことでハニーポットの検知を行うことが可能な HONEYBADGER と呼ばれるツールを発表している。しかし、この方式は特定のタイプのハニーポットに対する検知精度は高いが、新しいハニーポットを検知するのには適していな

[23] プログラムの実行パスに沿って分岐条件を採取してプログラムを模擬的に実行し、その結果を評価する手法。

い。

Camino *et al.* [2020] は、スマート・コントラクトに紐付く取引履歴を特徴量とする機械学習を用いたアプローチを提案している。ここでは、コントラクト、コントラクトの作成者、トランザクションの送信者、および他の参加者との間の資金移動を分析することで新しいハニーポットの検知を可能にしている。しかし、多くのスマート・コントラクト・ハニーポットは十分な取引記録を持っていないため、この方式は特徴抽出が困難であるという課題を持つ。特にこれらの研究では、取引履歴など被害者（低スキルの攻撃者）が暗号資産を盗み取られた後に取得可能な情報を活用しているため、実際に被害を抑えるためのモデルを構築できないという課題がある。

Chen *et al.* [2020] では、バイトコードにおいてオペコードの N-gram[24]に基づいたコントラクト・ハニーポットの検知手法を提案しており、新しいタイプの攻撃の検知も可能である。この手法は、コントラクトがデプロイされた後、トランザクション発行に伴いコントラクトが実行される際の情報も活用して特徴抽出を行うものであり、コントラクト実行時の振る舞いに共通性がある（例えば残高確認）ことから、スマート・コントラクト・ハニーポットの早期検知が可能である。しかし、依然としてコントラクトの実行前では特徴を抽出できないため、これも被害を抑えるためのモデルを構築できているとはいえない。原・高橋・面［2021］では、スマート・コントラクトを実行しなくても抽出できる特徴を活用する。具体的には、バイトコードから直接的に抽出した特徴のほか、コントラクトのデプロイ後にすぐ入手可能な SourceCode カテゴリ（コードの行数やコンパイラの種類など）を合わせた特徴を使用している。ゆえに、この方式はスマート・コントラクトを一度も実行せずに検知できるためデプロイ直後でも検知が可能となり、これまで研究されてきた手法よりも早期に検知できるという特徴を持つ。

５．ブロックチェーンに内在するセキュリティ・リスク

ブロックチェーンは非中央集権的な P2P ネットワークで構成されている。そのため、特定の組織によってブロックチェーンが統制されているわけではなく、ローンチされると基本的には動作し続けるように設計されている。つまり、ブロックチェーン・サービスが使われなくなったとしてもブロックチェーンを強制的に終了できない。その結果、ネットワーク・ノードがメンテナンスされずに放置されることで端末にサイバー攻撃を受けるリスクが生じる。また、ネットワーク・ノードが分散配置されていると信じられているが、実際にはノードの分散性が高く保たれているかどうかは不明である。ノードの分散性が低くなって

[24] 任意の文書などにおける連続する N 個の単語や文字のまとまりを表すもの。

特定の地域に偏ることになれば、ブロックチェーンのセキュリティ特性の 1 つである可用性の低下につながる。このように、ブロックチェーンには、ブロックチェーン・サービスが使われなくなったとしても完全に終了されないリスクやネットワーク・ノードの分散性が低下するリスクが存在するといえる。一般にブロックチェーン・サービスは暗号資産とともに使われることが多いため、暗号資産に価値がなくなるとサービスが機能しなくなる。これは、知名度の低いマイナーな暗号資産に限った話とはいえない。Bitcoin や Ethereum など知名度が高い主要な暗号資産においても、将来的に陳腐化が進んだとき、同様にブロックチェーン・サービスが使われなくなったとしてもブロックチェーンを終了することが難しいリスクやネットワーク・ノードの分散性が低下するリスクが存在する。

アルトコインを含めたさまざまな規模の暗号資産ブロックチェーンを分析することによって、ブロックチェーンに内在するセキュリティ・リスクを明らかにできると期待される。ここでは、マイナーな暗号資産および時価総額がゼロである無価値[25]な暗号資産に着目する。まずは無価値な暗号資産を対象とし、ブロックチェーン・サービスで使われている暗号資産に価値がなくなっているにもかかわらず、そのサービスの終了が困難であるリスクについて述べる。さらに、暗号資産の市場価値の高低によってサービス終了困難性リスクが変わるのかどうかについても考察する。次に、主要な暗号資産と比較して、マイナーな暗号資産のブロックチェーン・ネットワークの分散性が低下するリスクについて述べる。

（1）ブロックチェーン・サービスの終了困難性

ブロックチェーンの P2P ネットワークの十分な分散性により、暗号資産ネットワーク・システムの可用性が確保される。しかし、逆にその可用性のためにブロックチェーン・サービスを簡単に終了できないという問題がある。たとえ暗号資産の市場価値が無くなったとしても、そのブロックチェーン・データはブロックチェーン・アプリケーションと共に P2P ネットワーク上に残り続けることになる。一般に時間経過と共にアプリケーションに脆弱性が発見されアップデートが必要になる。もしアプリケーションがオフラインであれば放置してもそれほど問題ないかもしれないが、オンラインアプリケーションの場合メンテナンスせずに放置すると、脆弱性の放置につながるため端末にサイバー攻撃を受けるリスクが生じる。

Taguchi and Omote [2021]では、CryptoID[26]が 2020 年 6 月時点で取り扱っていた

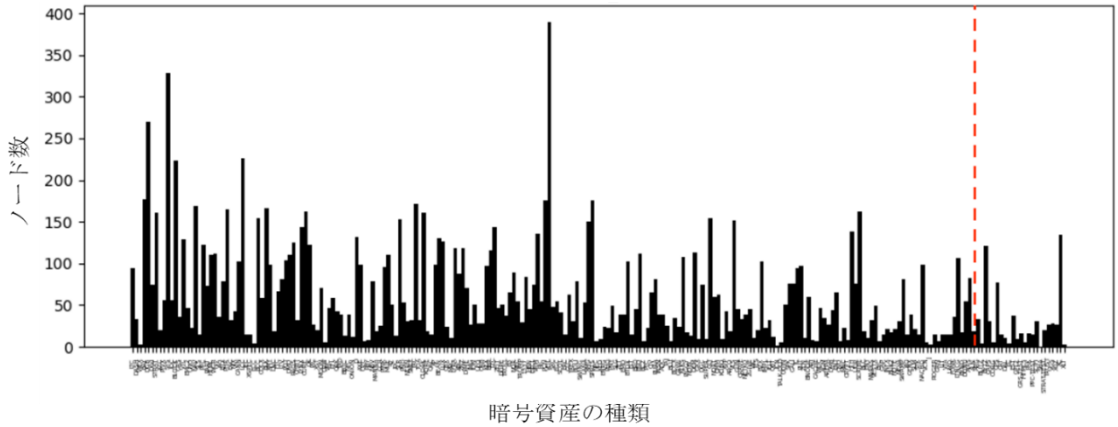
---

25 暗号資産は法定通貨と交換できてこそ（時価総額が存在してこそ）価値が認められるものである。本稿では、時価総額がゼロの暗号資産を「無価値な暗号資産」と定義する。

26 https://chainz.cryptoid.info/

238 銘柄を調査対象とし、各銘柄の USD 時価総額とネットワーク・ノード数を取得し、無価値な暗号資産ネットワークにノードが残存していることを確認している。具体的には、まず、市場価格が存在する暗号資産（213 銘柄）と無価値な暗号資産（25 銘柄）が存在していることを確認した。図 8 では、横軸が時価総額を降順に並べた銘柄、縦軸がノード数を表したグラフを示している。時価総額が存在する暗号資産と存在しない銘柄の境界はグラフ右部の破線で示しており、破線右側に無価値な暗号資産が存在していることがわかる。全 238 銘柄に対し市場価格を持たない銘柄が 25 件（12%）となっており、無価値な銘柄群の内ノードが存在する割合は 25 件中 24 件（96%）と概ねすべての無価値な銘柄にノードが残存していることが明らかになった。市場価値がある銘柄群に関しては価値がある銘柄 213 件すべてにノードが存在していた。なお、市場価値のない銘柄については銘柄のシンボル順で並べている。

図 8　マイナーな暗号資産（238 銘柄）のノード数



備考：横軸は暗号資産の種類の判別が不可能となるように表記している（原図のまま）。

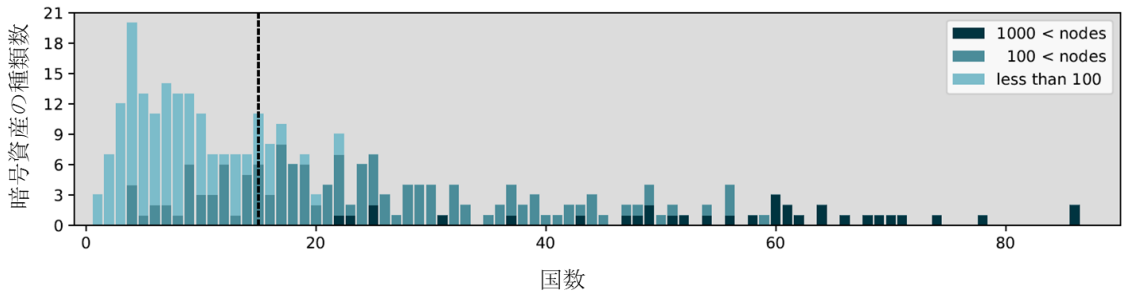
資料：Taguchi and Omote [2021]

さらに Taguchi and Omote [2021] では、調査対象の暗号資産 238 銘柄の時価総額と悪性判定数に相関が見られないかの調査を行っている。ここで悪性判定数には、VirusTotal によって悪性と判定された数を用いており、具体的にはノード当たりの平均悪性判定数を採用している。攻撃者にとって、市場価値の高い暗号資産が攻撃対象になりやすいのか、あるいはネットワーク・ノードが放置されていると見られる無価値な暗号資産が何らかの理由で攻撃対象になるのかのどちらも考えられる。結果としては、暗号資産の時価総額と悪性判定数に特に相関は見られていない。したがって、攻撃者がノードを攻撃するメリットは時価総額の高い銘柄と低い銘柄の両方に存在し、時価総額が低い銘柄にも、時価総額が高い銘柄と同じくらい攻撃が行われていたという新しい発見が得られた。

（２）ブロックチェーン・ネットワークのおける分散性低下のリスク

マイナーな暗号資産の多くは Bitcoin や Ethereum よりもネットワークの規模が小さいため、そのリスクも異なると考えられる。Imamura and Omote [2021] では、マイナーな暗号資産の特徴やリスクを分析している。具体的には、2020 年 5 月から 8 月までの期間で、CryptoID などが取り扱っていた 317 銘柄を調査対象とし、各暗号資産のノード数とノードが存在する国および ASN（Autonomous System Numbers）を取得している。このデータに基づき、マイナーな暗号資産におけるネットワーク・ノード数の規模が小さくなるにしたがって、分布する国数がどの程度減少するのかについて分析結果を示している。図 9 は、ノード数で見た暗号資産ネットワークの規模別に、ネットワーク・ノードが何ヵ国に跨がっているかを示したグラフである。1,000 ノード以上が存在する暗号資産ではノードが多くの国に分散しているが、100 ノード未満が存在する暗号資産ではノードが少数の国に偏っていることがわかる。また、棒グラフの高さが示すようにそうした暗号資産のほうが絶対数が多い。本研究により、ノード数で測った分散性が低下しているマイナーな暗号資産が数多く存在していることが明らかにされた。

図 9　ネットワーク・ノードが存在する国数と暗号資産の種類数の関係



資料：Imamura and Omote [2021]

６．おわりに

本稿では、ブロックチェーンの悪用に焦点をあて、非金融データの埋込みやスマート・コントラクトの実装上の仕組みを解説したうえで、C&C サーバやハニーポットといったネットワーク・セキュリティを解説した。これらの要素技術を踏まえて、ブロックチェーンへの攻撃、ブロックチェーンを悪用した攻撃、およびブロックチェーンに内在するセキュリティ・リスクについて最新の研究動向を紹介した。

ブロックチェーンの安全性である耐改ざん性と高可用性は、参加者にとって有用な性質であるが、それと同時に攻撃者にとっても魅力的な性質である。例え

ば、ブロックチェーン上に C&C サーバを構築することにより、攻撃者の命令は削除不可能であるだけでなく C&C インフラ自体を破壊することも不可能になるため、攻撃者は安心して Botnet を維持できるメリットがある。さらに、ブロックチェーンには、ブロックチェーン・サービスが使われなくなったとしても終了することが難しいというブロックチェーン特有のリスクが存在する。その結果、暗号資産のノードが放置され、端末がサイバー攻撃の温床になるといったリスクが考えられる。

このように、ブロックチェーンについて、暗号技術的な側面だけでなく、ネットワークに関連する側面からもその仕組みを理解し、サイバー攻撃やセキュリティ・リスクに備えることは極めて重要である。暗号資産を利用する者にとって、本稿の内容から具体的に以下の点に留意すべきであると考える。

- ブロックチェーン・ポイズニング攻撃により、送金情報以外の情報は汚染されている可能性がある。そのため、ブロックチェーン内の送金情報とそれ以外を明確に区別し、送金情報以外の情報を容易に信じないことが必要である。
- ブロックチェーンへのサイバー攻撃、ブロックチェーンの C&C サーバ化、スマート・コントラクト・ハニーポットにより、残高のある一般ユーザのウォレットが狙われているだけでなく、接続してくるユーザを待ち伏せする不正なスマート・コントラクトが存在していることも留意しておくことが重要である。
- ブロックチェーン・サービスの終了困難性、ブロックチェーン・ネットワークにおける分散性低下のリスクにより、ブロックチェーンの安全性が未来永劫続くものではなく、例えばネットワーク・ノード数が減少することによりセキュリティ・リスクが増大することに留意し、ブロックチェーンならば安全であると安易に考えないことが重要である。

【参考文献】

芦澤奈実・矢内直人・クルーズ・ジェイソン・ポール・岡村真吾、「Eth2Vec: 深層学習による言語処理に基づいたスマートコントラクトの安全性解析ツールの設計」、『コンピュータセキュリティシンポジウム 2020 論文集』、情報処理学会、2020 年、494～501 頁

王　佳・佐々木貴之・面　和成・吉岡克成・松本　勉、「Etherpot : イーサリアムのクライアントへのサイバー攻撃を観測するためのハニーポット」、『信学技報』121 巻 69 号、電子情報通信学会、2021 年、56～61 頁

木村圭吾・今村光良・面　和成、「NFT の信頼性にみるセキュリティリスクの考察」、『信学技報』121 巻 118 号、電子情報通信学会、2021 年、123～130 頁

———・面　和成、「ブロックチェーンの汚染による悪用リスクの考察」、『コンピュータセキュリティシンポジウム 2020 論文集』、情報処理学会、2020 年、963～970 頁

陳　浩太・面　和成、「Ethereum ネットワークにおけるハニーポット設置に向けた攻撃活動の分析」、『信学技報』120 巻 411 号、電子情報通信学会、2021 年、265～272 頁

原　和希・高橋健志・面　和成、「Ethereum におけるスマートコントラクトハニーポット検出のための Solidity バイトコードを活用した機械学習モデルの検討」、『2021 年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2E2-3、2021 年

Ali, Syed Taha, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao, “ZombieCoin: Powering Next-Generation Botnets with Bitcoin,” Proceedings of the 19th International Conference on Financial Cryptography and Data Security, LNCS, 8976, Springer-Verlag, 2015, pp. 34-48.

———, ———, ———, and ———, “ZombieCoin 2.0: Managing Next-Generation Botnets Using Bitcoin,” International Journal of Information Security, 17(4), 2018, pp. 411-422.

Böck, Leon, Nikolaos Alexopoulos, Emine Saracoglu, Max Mühlhäuser, and Emmanouil Vasilomanolakis, “Assessing the Threat of Blockchain-Based Botnets,” APWG Symposium on Electronic Crime Research, IEEE, 2019, pp. 1-11.

Buterin, Vitalik, “Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform,” 2013 (available at https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf、2021 年 10 月 10 日).

Camino, Ramiro, Christof Ferreira Torres, Mathis Baden, and Radu State, “A Data

Science Approach for Detecting Honeypots in Ethereum," Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency, IEEE, 2020, pp. 1–9.

Chen, Weili, Xiongfeng Guo, Zhiguang Chen, Zibin Zheng, Yutong Lu, and Yin Li, "Honeypot Contract Risk Warning on Ethereum Smart Contracts," Proceedings of the IEEE International Conference on Joint Cloud Computing, IEEE, 2020, pp. 1–8.

Cheng, Zhen, Xinrui Hou, Runhuai Li, Yajin Zhou, Xiapu Luo, Jinku Li, and Kui Ren, "Towards a First Step to Understand the Cryptocurrency Stealing Attack on Ethereum," Proceedings of the 22nd International Symposium on Research in Attacks, Intrusions and Defenses, USENIX, 2019, pp. 47-60.

Hara, Kazuki, Teppei Sato, Mitsuyoshi Imamura, and Kazumasa Omote, "Profiling of Malicious Users Targeting Ethereum's RPC Port Using Simple Honeypots," Proceedings of the 3rd IEEE International Conference on Blockchain, IEEE, 2020, pp. 1-8.

Imamura, Mitsuyoshi, and Kazumasa Omote, "Investigation and Analysis of Features in Decentralized Network Management of Minor Cryptocurrencies," Proceedings of the 35th IEEE International Conference on Advanced Information Networking and Applications, LNNS, 225, Springer-Verlag, 2021, pp. 245-258.

Kiffer, Lucianna, Dave Levin, and Alan Mislove, "Analyzing Ethereum's Contract Topology," Proceedings of the Internet Measurement Conference, ACM, 2018, pp. 494-499.

Li, Xiaoqi, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen, "A Survey on the Security of Blockchain Systems," Future Generation Computer Systems, 107, 2020, pp. 841-853.

Luu, Loi, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor, "Making Smart Contracts Smarter," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 254-269.

Matzutt, Roman, Martin Henze, Jan Henrik Ziegeldorf, Jens Hiller, and Klaus Wehrle, "Thwarting Unwanted Blockchain Content Insertion," Proceedings of the IEEE International Conference on Cloud Engineering, IEEE, 2018a, pp. 364-370.

———, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Mullmann, Oliver Hohlfeld, and Klaus Wehrle, "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin," Proceedings of the 22nd International Conference on Financial Cryptography and Data Security, LNCS, 10957, Springer-Verlag, 2018b, pp. 420-438.

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009 (available at https://bitcoin.org/bitcoin.pdf、2021 年 10 月 10 日).

Park, Sehyun, Seongwon Im, Youhwan Seol, and Jeongyeup Paek, “Nodes in the Bitcoin Network: Comparative Measurement Study and Survey,” IEEE Access, 7, IEEE, 2019, pp. 57009-57022.

Pletinckx, Stijn, Cyril Trap, and Christian Doerr, “Malware Coordination Using the Blockchain: An Analysis of the Cerber Ransomware,” Proceedings of 2018 IEEE Conference on Communications and Network Security, IEEE, 2018, pp. 1-9.

Sato, Teppei, Mitsuyoshi Imamura, and Kazumasa Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain,” Proceedings of the 13th WISTP International Conference on Information Security Theory and Practice, LNCS, 12024, Springer-Verlag, 2019, pp. 139-154.

Steiner, Jutta, “Security Advisory [Insecurely configured geth can make funds remotely accessible],” Ethereum Foundation Blog, 2015 (available at https://blog.ethereum.org、2021 年 10 月 10 日).

Taguchi, Wataru, and Kazumasa Omote, “Risk Analysis for Worthless Crypto Asset Networks,” Proceedings of the 35th IEEE International Conference on Advanced Information Networking and Applications, LNNS, 226, Springer-Verlag, 2021, pp. 592-602.

Torres, Christof Ferreira, Mathis Steichen, and Radu State, “The Art of the Scam: Demystifying Honeypots in Ethereum Smart Contracts,” Proceedings of the 28th USENIX Security Symposium, USENIX, 2019, pp. 1591-1607.

Tsankov, Petar, Andrei Dan, Dana Drachsler-Cohen, Arthur Gervais, Florian Bünzli, and Martin Vechev, “Securify: Practical Security Analysis of Smart Contracts,” Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, ACM, 2018, pp. 67-82.

Zhang, Mengya, Xiaokuan Zhang, Yinqian Zhang, and Zhiqiang Lin, “TXSPECTOR: Uncovering Attacks in Ethereum from Transactions,” Proceedings of the 29th USENIX Security Symposium, USENIX, 2020, pp. 2775-2792.