Computer Security Symposium 2020
26 - 29 October 2020

アニーリング計算を用いた マルウェア感染ネットワークの遮断最適化

山口 純平[1,a)]　清水 俊也[1]　古川 和快[1]　鳥居 悟[1]　森川 郁也[1]　伊豆 哲也[1]

概要：近年，量子アニーリング計算機や疑似的に量子アニーリングを再現するアニーリング計算機の開発が進んでおり，実用的な規模の組合せ最適化問題を解くことが可能となりつつある．セキュリティの分野においても応用研究が進められており，汎用計算機を超えない範囲ではあるが暗号解析で成果が出始めている．これらのノウハウを元に，我々はアニーリング計算機のさらなる応用として，サイバーセキュリティの課題である「マルウェア感染ネットワークの通信路遮断最適化問題」の単純化したモデルを設計し，これに対してアニーリング計算機を適用した．この中で我々は，従来のように最適化問題を既知の組合せ最適化問題に帰着させるのではなく，実問題に近い形で独自の定式化を与えた．また，富士通のアニーリング計算機であるデジタルアニーラ（DA）を用いた本定式化の求解実験では，全数探索の計算量が 2^{5246} となる 219 台の PC・サーバが接続されたネットワークの遮断最適化問題に対して，自明な解より最適な遮断の組合せを計算できた．

キーワード：アニーリング，遮断最適化問題

Solving Malware-Infected Network Disconnection Optimization Problems using Annealing Computation

Junpei Yamaguchi[1,a)]　Toshiya Shimizu[1]　Kazuyoshi Furukawa[1]　Satoru Torii[1]
Ikuya Morikawa[1]　Tetsuya Izu[1]

Abstract: Recently, annealing computers including quantum annealing computers and digital computers specialized for annealing computation inspired by the quantum annealing have been developed, and the time is approaching when these computers can solve practical-scale combinatorial optimization problems. Although these computers have not reached general computers, they are applied to security fields such as cryptanalysis. With knowledge of these studies, we apply them to a simplified model of “malware-infected network disconnection optimization problem” as a further application. In this study, we give a formulation of the problem close to reality, not attributing the problem to known combinatorial optimization problems. In our experiments using the Digital Annealer developed by Fujitsu, we tried to solve a problem which has a network with 219 PC/Server connections and 2^{5246} complexity in exhaustive search and succeeded in finding a solution of the problem better than that of the trivial solution.

Keywords: Annealing, Disconnecting optimization problem

1. はじめに

近年，量子アニーリング計算機とそれをデジタル回路で疑似的に再現するアニーリング計算機が盛んに開発されており，実用的な規模の組合せ最適化問題を解くことが可能になってきている．これらの計算機はイジングモデル（つまりバイナリ変数からなる 2 次多変数多項式）を受け取り，その最小値を効率的に探索することができる．ナップサック問題や巡回セールスマン問題などの代表的な組合せ

[1] 株式会社富士通研究所 セキュリティ研究所
Security Laboratory, Fujitsu Laboratories Ltd.
[a)] j-yamaguchi@fujitsu.com

最適化問題に対しては，そのイジングモデルへの定式化方法が既に知られており [1]，アニーリング計算機によって解くことが可能となっている．これを利用して，例えば物流の分野では配送の最適化，製造の分野では生産計画の最適化など一部ではすでに業務の効率化に応用されている．一方，セキュリティの分野でもアニーリング計算機が活用されており，例えば暗号解析に用いられている．共通鍵暗号では，AES の差分特性探索の解析 [2] に，また公開鍵暗号では，RSA 暗号の素因数分解問題 [3], [4], [5]・多変数多項式暗号の MQ 問題 [6]・格子暗号の格子問題 [7], [8] の求解に応用されている．例えば，素因数分解問題では 30bit 合成数の素因数分解に成功しており，格子問題では低次元ではあるが最短ベクトル問題の求解に成功している．このようにまだ限られた範囲ではあるが，セキュリティ分野においてアニーリング計算機の活用が検討されはじめている．

我々は新たにサイバーセキュリティの分野でアニーリング計算機を活用するために，その一試行として，マルウェア感染ネットワークの遮断最適化問題にアニーリング計算機を適用した．組織内ネットワークがマルウェアに感染したとき，さらなる感染を防ぐには感染端末をネットワークから隔離したり，ネットワーク全体をインターネットから遮断したり等，ネットワーク遮断の対応を取ることが一般的である．しかし業務・ビジネスを継続させるという観点から見ると，ビジネス的な損失につながるネットワーク遮断はできるだけ最小限にすることが要求される．つまり，マルウェア感染時には，ネットワークのどこを接続してどこを遮断するかという組合せ要素を媒介して，さらなる感染リスクとビジネス損失のトレードオフが存在する．このトレードオフにおいて最適解を計算する問題をマルウェア感染ネットワークの遮断最適化問題とする．

2015 年に情報漏洩が起こった日本年金機構のマルウェア感染事例 [9] に代表されるように，現在はマルウェア感染時の初動として感染端末の隔離を行い，それでも感染を食い止められない場合にはネットワーク全体をインターネットから隔離するという対策を取るのが一般的である．我々はこのような事例のように，ビジネス損失を軽視して一律にセキュリティを高くする，つまりさらなる感染リスクを下げる方向に倒しきるのではなく，ある程度はリスクを受け入れてビジネス損失を減少させることでマルウェア被害をより最小にできるのではないかという新しいセキュリティのあり方を考えた．しかし現代のネットワーク構造は非常に複雑であり，これまでの計算機では組合せ爆発によりネットワーク遮断最適化問題を求解することは難しい．そこで組合せ最適化計算に特化させたアニーリング計算機であれば解決できる可能性があると考え，本問題に取り組んだ．

組織内ネットワークにおいて，さらなる感染リスクや遮断による損失を考えるには，ネットワーク内のすべての機器に保存されている情報の価値や，すべての機器間の通信量や通信監視センサの有無等の情報を正確に把握し数値化する必要がある．しかし，現在の技術ではこれを実現することは困難である．そこで本稿では，これらの数値化がすでにできていると仮定するネットワーク遮断最適化問題の単純化モデルを構築した．そして，このモデル化に対してイジングモデル定式化を与え，富士通のアニーリング計算機であるデジタルアニーラ（DA）を用いて本問題の求解を行った．特に，定式化においては既存の組合せ最適化問題に帰着させるのではなく，より現実の問題に近くなるよう独自の定式化を与えている．求解実験では，全数探索の計算量が 2^{5246} となる 219 台の PC・サーバが接続されたネットワークの遮断最適化問題に対して，自明な解より最適な遮断の箇所の組合せの計算に成功した．本試行により，ネットワーク遮断最適化にアニーリング計算機の実応用の可能性を確認することができた．

2. アニーリング

ここでは，アニーリング計算と次数削減法について紹介する．

2.1 ハミルトニアン

D-Wave 2000Q や富士通の DA などのアニーリング計算機の目的は，以下で示すイジングモデルのハミルトニアンの最小値を効率的に探索することである：

$$H(\mathbf{x}) = -\mathbf{x}^{\mathrm{T}}\mathbf{W}\mathbf{x} - \mathbf{b}^{\mathrm{T}}\mathbf{x} + c,$$

ここで $\mathbf{W} = (w_{i,j}) \in \mathbb{Z}^{n\times n}, \mathbf{b} \in \mathbb{Z}^n, c \in \mathbb{Z}$ かつ $\mathbf{x} \in \{0,1\}^n$ である．もし任意の $1 \leq i, j \leq n$ に対し $w_{i,j} \neq 0$ のとき，ハミルトニアンは全結合であるという．アニーリング計算は確率的アルゴリズムのため，アニーリング計算機は必ずしもハミルトニアンの最小値を計算するというわけではなく，しばしば局所解を出力する．

2.2 アニーリング計算機の規模

アニーリング計算機が扱えるハミルトニアンの大きさはハードウェア毎に異なっている．D-Wave 2000Q は 2048 量子ビットをもつが，それらはキメラ構造で接続されている．つまり，この計算機でハミルトニアンを解く場合，ハミルトニアンをキメラグラフに埋め込まなければならない．このとき，ハミルトニアンの 1 つの変数が複数の量子ビットに埋め込まれることがある．このため，D-Wave 2000Q は最悪の場合 64 変数のハミルトニアンまでしか扱うことが出来ない．一方で，量子アニーリングをデジタル回路で疑似的に再現したアニーリング計算機はより大きな規模が実現している．例えば，最新の DA であれば全結合かどうかにかかわらず 8192 変数までのハミルトニアンを扱うことができる [10]．また，CMOS は 102400 個のイジングス

ピンを要するが [11] それらは特殊な形で結合されているため，ハミルトニアンが全結合の場合は 319 変数までを扱うことができる [12].

2.3 アニーリング計算機の制限

アニーリング計算機はハミルトニアンの最小値探索しか行うことができない．したがって，ある問題をアニーリング計算機で解く場合，その問題をハミルトニアンに定式化しないといけない．ナップサック問題や巡回セールスマン問題などの有名な組合せ最適化問題はすでにで定式化が与えられている．またセキュリティの分野においては，素因数分解問題の求解，多変数多項式暗号の求解，最短ベクトル問題などの格子問題の求解，AES の差分特性探索の解析などに関するハミルトニアン定式化が知られている．

2.4 次数削減法

たいていの場合，解きたい問題を直接ハミルトニアンに変換することは難しい．このとき，その問題をいったん高次元多項式の最小値問題に帰着させ，次数削減法 [13], [14] を使ってその多項式を同じ最小解を持つハミルトニアンに変換するのが一般的である．

次数削減法のアイデアは 2 つのバイナリ変数の積を新たなバイナリ変数に置き換えることである．バイナリ変数からなる高次元多項式 E が与えられたとする．このとき，ふたつのバイナリ変数からなる多項式 f, g を用いて

$$E(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + x_i x_j g(x_1, \ldots, x_n),$$

と表せる．ただし g の次数は 1 以上である．ここで，新たなバイナリ変数を $x_{ij} := x_i x_j$ とし，新しい多項式を

$$E_1(x_1, \ldots, x_n, x_{i,j}) = f + x_{i,j} g + MP(x_i, x_j, x_{i,j})$$

とする．ここで $P = x_i x_j - 2x_i x_{i,j} - 2x_j x_{i,j} + 3x_{i,j}$ はペナルティ関数で $M = \max\{|g| + 1, 1\}$ である．このとき，もし $(X_1, \ldots, X_{n+1}) \in \{0,1\}^{n+1}$ が E_1 の最小解を与えるならば，$(X_1, \ldots, X_n)$ は E の最小解を与える．したがって，E_1 の最小解を計算することは E の最小解を計算することに等しい．この操作を再帰的に行うことで，もとの多項式 E を $n+m$ 変数を持つハミルトニアン E_m に変換することができる．ここで m は繰り返した操作の回数である．操作 1 回につき 1 変数増加するため，もし元の多項式 E の次元が大きい場合，得られるハミルトニアンの変数の数が多くなることに注意が必要である．また，もし元の多項式 E の次数が十分に大きい場合，この操作は計算量的に困難である．なぜならば，n 変数 k 次元多項式は最悪の場合 $\sum_{i=1}^{k} {}_nC_i (\geq 2^k)$ 個の項をもつからである．

3. ネットワーク遮断最適化問題

ここでは，マルウェア感染ネットワークの遮断最適化問題の単純なモデル化およびハミルトニアン定式化を提案する．

3.1 単純なモデル化

ネットワークの遮断最適化には，ネットワークに属する各機器がもつ資産の情報や権限の強さなどの機器に関する情報や，機器間の通信量や通信監視センサの設置有無等の通信路に関する情報など，非常に多くの情報が必要となる．本稿では，上記のような最適化に必要な情報がすでに入手できており，さらにこれらの情報が機器の資産価値，通信路の価値（以降，通信量とよぶ）というパラメータで表せていると仮定する．この仮定によりマルウェア感染ネットワークの遮断最適化問題は，ネットワーク構造・各機器の資産価値・各通信路の通信量を入力とし，最適なネットワークの遮断箇所の組合せを計算するという単純なモデルとして表すことが出来る．以降では，この単純なモデルをハミルトニアンに定式化する方法および第 2 世代 DA[15] を用いた求解実験の結果を紹介する．

3.2 準備

ネットワーク構造を，PC やサーバなどの機器を表す頂点集合 $V = \{v_1, \ldots, v_n\}$ とそれら機器間の接続を表す辺集合 E で構成される無向グラフ $G = (V, E)$ で表す．ある頂点 $v \in V$ を要素に持つ辺の集合全体を $Adj(v, E) = \{e \in E : v \in e\}$ で表す．また，異なる 2 つの頂点 $u, w \in V$ に対し，$\{u, v_1\}, \{v_1, v_2\}, \ldots, \{v_{k-1}, v_k\}, \{v_k, w\}$ が全て辺となるようなそれぞれが互いに異なる点の列 $v_1, \ldots, v_k \in V \setminus \{u, w\}$ が存在するとき，$P = (\{u, v_1\}, \{v_1, v_2\}, \ldots, \{v_{k-1}, v_k\}, \{v_k, w\})$ を u から w へのパスといい，パスに含まれる辺の数（この場合は $k+1$）をパス長と呼ぶ．さらに，異なる 2 つの頂点 $u, w \in V$ に対し，長さ t 以下のパス全体の集合を $Path(u, w, E, t)$ で表す．また，頂点には資産価値 $mv : V \to \mathbb{Z}_{\geq 0}$ が，辺には通信量 $w : E \to \mathbb{Z}_{\geq 0}$ が定義されているとする．ここで $\mathbb{Z}_{\geq 0}$ は 0 以上の整数全体の集合である．

3.3 定式化

ネットワーク構造のグラフ $G = (V, E)$ と資産価値・通信量を表す関数 mv, w およびマルウェアに感染したノード $v_0 \in V$ が与えられたとする．各辺 $e \in E$ に対してバイナリ変数 $x_e \in \{0,1\}$ を与え，0 なら遮断 1 なら接続と割り当てることで，ネットワークのどの辺を遮断してどの辺を接続するかをバイナリベクトル $\mathbf{x} \in \{0,1\}^{|E|}$ で表すことができる．ここでは，この $\mathbf{x}$ を用いてそのネットワーク構造に対するビジネス損失関数 $Loss(\mathbf{x})$ およびさらなる感染リスク関数 $Risk(\mathbf{x})$ を定義する．リスク関数に関しては，状況に応じて変更できるよう複数の定義を与える．

3.3.1　損失関数 $Loss$ の定義

辺 $e = \{v, w\} \in E$ を遮断したことにより生じる損失は，通信量 $w(e)$ の大きさおよび両端の資産価値 $mv(v), mv(w)$ の大きさに応じてその辺の両端である点 v, w に生じると考えるのが自然である．そこで，辺 e を遮断したことによる点 v に生じる損失を

$$L(v, e) \coloneqq cv(v, w) \times w(e) \times (1 - x_e)$$

と定義する．ここで，$cv : V^2 \to \mathbb{R}$ は価値係数であり，例えば資産価値の平均値 $V_{ave} \coloneqq \sum_{v \in V} mv(v)/|V|$ に対して

$$cv(v, w) = \frac{(mv(v) + mv(w))/2}{V_{ave}}$$

とするなど，$mv(v), mv(w)$ の大きさに依存して大きくなるようにすることで，重要な資産につながる辺を遮断することにより生じる損失が大きくなるように定義できる．また，$(1 - x_e)$ をかけることで，辺 e が遮断，すなわち $x_e = 0$ のときのみ損失が加算されるようになっている．辺 e を遮断したときに点 w に生じる損失も同様に定義される．

点 v に生じる損失 $L(v)$ は，v につながる全ての辺 $Adj(v, E)$ で生じる損失の総和と定義する．つまり，

$$L(v) = \sum_{e \in Adj(v, E)} L(v, e)$$

である．

最後に，ネットワーク全体に生じる損失は，感染端末を除いた全ての点に生じる損失の総和であると定義する．したがって，ネットワーク構造を表す $\mathbf{x}$ に対し損失関数は

$$Loss(\mathbf{x}) = \sum_{v \in V \setminus \{v_0\}} L(v)$$

で与えられる．

3.3.2　リスク関数 $Risk$ の定義

はじめに，感染端末 v_0 から他の端末 $v \in V$ に感染するリスクを考える．感染経路には，点 v_0 から v への全てのパスが考えられるが，長いパスが感染経路となることは考えにくい．そこで限界パス長 $T \leq |E|$ を定義し，感染経路として $Path(v_0, v, E, T)$ のみを考慮することにする．このうちパス長が $\ell \leq T$ のものを一つ選び，$P = (e_1, \ldots, e_\ell)$ とおく．このとき，パス P を通って v_0 から v に感染するリスク $R(P)$ は辺 $e_1, \ldots, e_\ell$ の通信量から算出されると考えるのが自然である．また，パス長が長いほど感染確率は低くなるため，パス長に応じて感染リスクを定義する必要がある．そこで我々は以下の 3 つのモデルを考えた．これらのモデルはネットワーク構造等の状況に応じて使い分ければよい．

最小値モデル　通信量の最小値を感染リスクとするモデル．すなわち，パス P の感染リスクは $M_1(P) \coloneqq \min_i w(e_i)$ で計算される．

軽減係数モデル　パスに含まれる辺の通信量の総和に対して，パス長に応じた軽減係数 $c(P)$ をかけるモデル．すなわちパス P の感染リスクは $M_2(P) \coloneqq c(P) \times \sum_{i=1}^{\ell} w(e_i)$ で計算される．

線形和モデル　軽減係数 $c_1 \geq \cdots \geq c_\ell$ に対して感染リスクを計算するモデル．パス P の感染リスクは $M_3(P) \coloneqq \sum_{i=1}^{\ell} c_i w(e_i)$ で計算される．

ここからは，上記モデルの計算方法 M_1, M_2, M_3 を関数 M で表す．このとき，パス P を通って v_0 から v に感染するリスク $R(P)$ を

$$R(P) = M(P) \prod_{i=1}^{\ell} x_{e_i}$$

で定義する．辺 $e_1, \ldots, e_\ell$ が全て接続，すなわち x_{e_i} が全て 1 のときのみ感染リスクが存在し，逆にひとつでも遮断された辺があるときは感染リスクが 0 になるようになっている．以上より，点 v_0 から v への感染リスクは，$Path(v_0, v, E, T)$ のすべてのパスで生じる感染リスクの総和で定義され

$$R(v_0, v) = \sum_{P \in Path(v_0, v, E, T)} R(P)$$

となる．

ネットワーク全体の感染リスクは，感染端末を除いたすべての点に生じるリスクの総和であると定義する．したがって，ネットワーク構造を表す $\mathbf{x}$ に対しリスク関数は

$$Risk(\mathbf{x}) = \sum_{v \in V \setminus \{v_0\}} R(v_0, v)$$

で与えられる．

3.3.3　遮断最適化問題のハミルトニアン

マルウェア感染ネットワークの遮断最適化問題の目的は，さらなる感染リスク $Risk(\mathbf{x})$ とビジネス損失 $Loss(\mathbf{x})$ の両指標が同時に小さくなるような $\mathbf{x}$ を計算することである．複数指標の最適化には，重み和を最小化する方法や各指標の最大値を最小化する方法などが知られている．今回は前者を採用し，$f(\mathbf{x}) \coloneqq Risk(\mathbf{x}) + Loss(\mathbf{x})$ を最小にするネットワーク構造 $\mathbf{x}$ をアニーリング計算で求めた．目的関数 $f(\mathbf{x})$ は限界パス長 T に対する T 次バイナリ多項式となっており，次数削減法を用いてハミルトニアンに変換することが可能である．以降，目的関数 f に次数削減法を適用して計算したハミルトニアンを H で表す．なお，以下の注意 1, 2 のように次数削減を行うと，得られるハミルトニアンの変数の数が少なくなるため効率的にアニーリング計算を行うことができる．また，例 3 にハミルトニアンの生成例を示す．

注意 1　次数削減法は出現頻度の多い変数の積に対して適用するのが効率的である．例として，3 次多項式を $g = x_1x_2x_3 + x_1x_2x_4$ とする．まず x_2x_3 を新たな変数 x_{23}

に置き換えた場合，1 つ目の項は 2 次式に変換できるが，2 つ目の項が 3 次のままのため，もう 1 度変数変換が必要となる．結果，g は 6 変数ハミルトニアンに変換される．一方，この多項式では x_1x_2 が共通項である．したがって x_1x_2 を x_{12} で置き換えることで，どちらの項も同時に 2 次式に変換することが可能である．このとき g は 5 変数ハミルトニアンに変換され，前の方法で次数削減したものよりもアニーリング計算が効率的となる．

注意 2　遮断最適化問題では，感染端末 v_0 に近い辺の変数の出現頻度が大きくなるため，これらの変数の積から順に次数削減をすると効率が良い．例えば，2 つの辺 $e_1 = \{v_0, v_1\}, e_2 = \{v_1, v_2\}$ を固定する．点 v_0, v_1 以外に v_2 に対して辺が存在する点を $v_3, \ldots, v_k$ とし，それぞれの辺を $e_3, \ldots, e_k$ とする．このとき，目的関数 $f(\mathbf{x})$ は少なくとも $x_{e_1}x_{e_2}(M(e_1, e_2, e_3)x_{e_3} + \cdots + M(e_1, e_2, e_k)x_{e_k})$ という 3 次の項を持つ．したがって，$x_{e_1}x_{e_2}$ に対して次数削減を行うと効率的である．

例 3　図 1 のネットワークに対して損失関数・リスク関数を計算する．まず損失関数を計算する．機器 X には辺 e_1, e_2 が接続されており，それらを遮断することにより X に生じる損失はそれぞれ $L(X, e_1) = 48(1 - x_1), L(X, e_2) = 32(1 - x_2)$ となる．したがって，機器 X に生じる損失は $L(X) = L(X, e_1) + L(X, e_2) = -48x_1 - 32x_2 + 80$ となる．同様に $L(B), L(Y)$ を計算することで，$Loss(\mathbf{x}) = L(X) + L(B) + L(Y) = -96x_1 - 32x_2 - 272x_3 - 48x_4 - 84x_5 + 532$ を得る．次にリスク関数を計算する．ここでは最小値モデルを採用し，限界パス長は $T = 3$ とする．機器 A から機器 X へのパスは $e_2, (e_4, e_1), (e_5, e_3, e_1)$ の 3 つであり，それぞれの経路により生じる感染リスクはそれぞれ $50x_2, 50x_1x_4, 60x_1x_3x_5$ である．したがって機器 X の感染リスクは $R(A, X) = 50x_2 + 50x_1x_4 + 60x_1x_3x_5$ となる．同様に $R(B), R(Y)$ を計算することで，$Risk(\mathbf{x}) = 50x_2 + 50x_4 + 70x_5 + 50x_1x_4; 50x_1x_2 + 70x_3x_5 + 50x_3x_4 + 50x_1x_2x_3 + 60x_1x_3x_5$ を得る．目的関数は $f(\mathbf{x}) = Loss(\mathbf{x}) + Risk(\mathbf{x})$ で計算されるが，これは 3 次多項式である．そこで $x_6 := x_1x_2, x_7 := x_1x_3$ と変換することで次数削減法により，新たな $\mathbf{x} = (x_1, \ldots, x_7)^{\mathrm{T}}$ に対してハミルトニアン $H(\mathbf{x}) = -\mathbf{x}^{\mathrm{T}}\mathbf{W}\mathbf{x} - \mathbf{b}\mathbf{x} + 532$ を得る．ただし，

$$\mathbf{W} = \begin{pmatrix} 0 & -101 & -61 & -50 & 0 & 102 & 122 \\ 0 & 0 & 0 & 0 & 0 & 102 & 0 \\ 0 & 0 & 0 & -50 & -70 & 0 & 122 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{Z}^{7\times 7},$$

$$\mathbf{b} = \begin{pmatrix} 96 & -18 & 272 & -2 & 14 & -153 & -183 \end{pmatrix} \in \mathbb{Z}^{7},$$

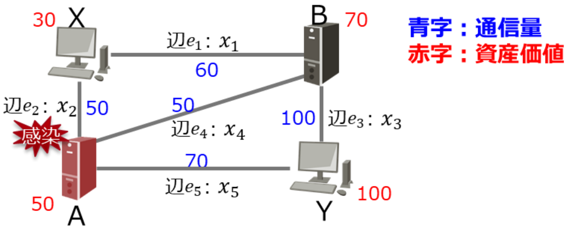

図 1　例 3 のネットワーク構成図

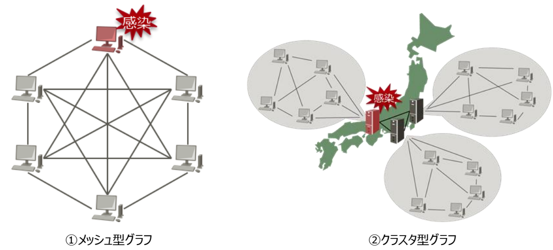

図 2　メッシュ型グラフとクラスタ型グラフのイメージ図

である．

4. 実験結果

ここでは，富士通のアニーリング計算機である第 2 世代 DA[15] を使った遮断最適化問題の求解結果を示す．

4.1 解の基準

遮断最適化問題の一般的な対応として，感染端末に接続する辺を全て遮断してしまう全遮断と，どの辺も遮断しない全接続とがある．これらを自明な解と呼ぶ．本稿では，「遮断最適化問題が解けた」とは，アニーリング計算によって自明な解に対応する目的関数 $f(\mathbf{x})$ の値より真に小さい値を与える解を発見できたことをいい，その解を最適解と呼ぶ（つまり最適解は複数存在することがある）．また $f(\mathbf{x})$ の最小値を与える解を最小解と呼ぶ．

4.2 想定ネットワーク構造

今回，ネットワーク構造として図 2 のようにメッシュ型グラフとクラスタ型グラフの 2 種類に対して実験を行った．メッシュ型グラフは，ノード（PC やサーバ同士）が相互に密に通信を行うモデルであり，会社の 1 拠点内のネットワークを想定している．メッシュ型グラフ内のノードの数をノード数といい，N で表す．一方，クラスタ型グラフは複数のメッシュ型グラフが代表ノードを介して通信を行うモデルであり，複数の拠点（クラスタ）を持つような大きな会社のネットワークを想定している．クラスタ型グラフにおいて，クラスタの数を C とし，ノードの総数をノード数と呼び N で表す．本稿では，$C = 3$ とし，各クラスタ内のノードは同数とした．つまり，各クラスタはそれぞれ $N/3$ 個のノードを持つ．

4.3 DA による実験結果

メッシュ型グラフ・クラスタ型グラフのそれぞれに対する遮断最適化問題の実験結果を示す．

4.3.1 メッシュ型グラフに対する実験

実験は以下の手順で，ノード数 N を大きくしながら複数回行った．

(1) ノード数 N のメッシュ型グラフのネットワークを次のように構成する．まず，感染ノードを 1 つ決定する．次に，各ノード v の資産価値 $mv(v)$ を 1 から 1100 の整数値で一様ランダムに割り当てる．また，各辺 e の通信量 $w(e)$ を 1 から 100 の整数値で一様ランダムに割り当てる．最後に各辺 $e = \{v, w\}$ の価値係数 $cv(v, w) = (mv(v) + mv(w))/1100$ を計算する．

(2) 限界パス長を $T = 3$ とし，最小値モデルを用いてハミルトニアン $H(\mathbf{x})$ を計算する．

(3) アニーリング計算機（DA）を用いて $H(\mathbf{x})$ を小さくする解を求める．

上記実験で DA は，ノード数 N によらず全ての実験で自明な解である全遮断を出力した．

メッシュ型グラフでは感染経路となるパスが非常に多く，辺の遮断により生じる損失の割に感染リスクが高くなる傾向があるため，基本的には全遮断が最小解となる．つまり DA は正しくハミルトニアンの最小解を計算できていることがわかる．

4.3.2 クラスタ型グラフに対する実験

はじめに例として，ノード数 $N = 30$ において DA が計算した最適解（図中の黒線は接続，赤線は遮断）を図 3 に示す．図中の○はノード，ノード同士をつなぐ辺はネットワーク通信路を表しており，○の中の数字はノードの番号である．特に，N1・N11・N21 は各クラスタの代表ノードであり，N1 が感染ノードである．各ノードの資産価値，各辺の通信量の具体的な値については本稿後半の付録 A.1 で紹介する．本ネットワークの通信路の数（辺の数）は 80 本のため，全数探索で最小解を計算するには 2^{80} の計算量が必要となる．なお，このネットワークに対するハミルトニアンの変数の数は 113 であった．自明な解である全遮断・全接続の目的関数 $f(\mathbf{x})$ の値はそれぞれ 13773 $(= 13773 + 0)$ と 14268 $(= 0 + 14268)$ であった（括弧内はそれぞれ $Loss(\mathbf{x}), Risk(\mathbf{x})$ の値）．一方，DA の最適解の値は 11164 $(= 6599 + 4565)$ であり，リスクと損失がバランス化されその和は自明な解よりも真に小さいものとなった．また，DA がこの最適解を計算するのにかかった時間は 1 秒以下であった．このようにアニーリング計算機を適用することで現状の計算機では時間がかかる計算量を持つ問題の最適なネットワーク遮断箇所の組合せをリアルタイムに計算することが可能であることがわかった．

次に，ノード数をより大きくして実験を行った．実験の詳細は下記の通りである．特に，パラメータ設定が現実に

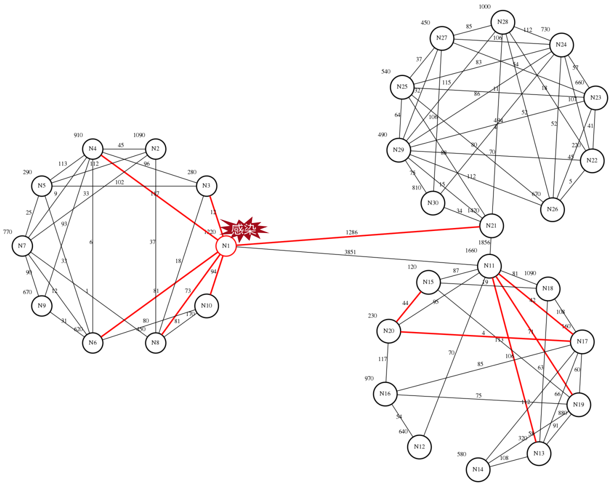

図 3 ノード数 $N = 30$ のクラスタ型グラフに対する DA の最適解．赤色の辺が遮断する辺で，黒色の辺が接続する辺を表す．

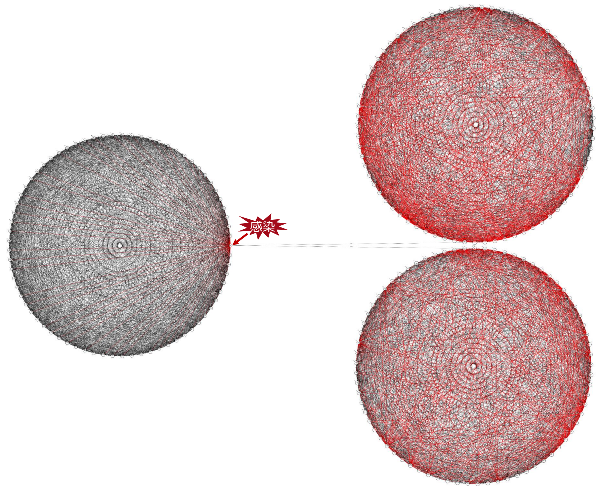

図 4 ノード数 $N = 219$ のクラスタ型グラフに対する DA の最適解．赤色の辺が遮断する辺で，黒色の辺が接続する辺を表す．

近づくよう，資産価値は代表ノードがその他ノードより大きくなるように，通信量は代表ノード間，代表ノードとその他ノード間，代表ノードではないその他のノード間の順に大きくなるように設定を工夫した．

(1) ノード数 N のクラスタ型グラフを以下のように生成する．まず，辺の密度が 67%程度になるように（つまり各クラスタ内において ${}_{N/3}C_2 * 2/3$ 本程度の辺が存在するように設定し）N ノードのクラスタ型グラフをランダムに生成する．次に，各ノード v の資産価値 $mv(v)$ を $10, 20, \ldots, 110$ の中から一様ランダムに割り当てる．ただし，代表ノードはさらに +200 とする．また，代表ノード間の通信量は $150 * N/3$ 程度の整数値をランダムに，代表ノードとその他のノード間の通信量は $10, 20, \ldots, 110$ の中から一様ランダムに，代表ノードではないノード間の通信量は $5, 6, \ldots, 15$ の中から一様ランダムに割り当てた．最後に各辺 $e = \{v, w\}$ の価値係数 $cv(v, w) = (mv(v) + mv(w))/110$ を計算

表 1　クラスタ型グラフに対する実験結果一覧

Node	辺の数	変数	自明な解	DA の解	「DA の解 < 自明な解」か
162	2875	4324	84713	79101	○
165	2960	4356	90596	82916	○
168	3110	4798	88260	87466	○
171	3249	4703	98460	87980	○
174	3329	5135	94893	90215	○
177	3441	5359	99597	92711	○
180	3553	5554	97716	91957	○
183	3676	5352	110709	97725	○
186	3817	5853	94410	91450	○
189	3909	5656	118521	105172	○
192	4017	6185	101677	103551	×
195	4147	6230	103240	101679	○
198	4290	6120	121803	112388	○
201	4413	6543	108243	111170	×
204	4532	6785	126498	118773	○
210	4828	7041	104043	124238	×
213	4954	7251	118964	122810	×
216	5116	7336	134796	128661	○
219	5264	8075	91207	90444	○

する．

(2) 限界パス長を $T = 3$ とし，最小値モデルを用いてハミルトニアン $H(\mathbf{x})$ を計算し，DA を使って解を計算する．

ノード数 $N = 162, 165, \ldots, 219$ の実験結果を表 1 に示す．DA を用いることで，19 件の実験中 $N = 192, 201, 210, 213$ を除く 15 件で最適解の計算に成功した．全ての実験において，DA の計算時間はおよそ 4 秒であった．

DA で求解できた遮断最適化問題のうち最もノード数が大きいものを図 4 に示す．黒色が接続する辺であり，赤色が遮断する辺を表している．ノード数は $N = 219$ であり，各クラスタにノードが 73 ずつ存在している．図中の辺の数は 5246 本であり，全数探索で最小解を計算するには 2^{5246} の計算量が必要となるため，汎用 PC で全数探索により最小解を計算するのは計算量的に困難である．なお，ハミルトニアンの変数の数は 8075 であり，現状の DA の限界である 8192 ビットのほとんどを使用している．アニーリング計算機はまだまだ発展途上であり，今後もビット数・計算速度が向上することを考えると，将来的にはさらに大規模な問題でも数秒程度で最適解が計算できると期待できる．

5.　おわりに

本稿では，セキュリティの分野でアニーリング計算機をさらに活用することを狙って，サイバーセキュリティの課題であるマルウェア感染ネットワークの遮断最適化問題を単純化したモデルを設計し，アニーリング計算機を適用した．また，モデルの定式化においては，既知の組合せ最適化問題に帰着させるのではなく，現実課題に即した独自の定式化を与えた．富士通のアニーリング計算機であるデジタルアニーラ（DA）を用いた実験では，全数探索の計算量が 2^{5246} となるノード数 219 のネットワーク遮断最適化問題において，自明な解である全遮断・全接続より最適なネットワーク遮断箇所の組合せの計算に成功した．この実験で生成されたハミルトニアンの変数の数は 8075 であり，現在の DA が扱うことのできる最大ビットである 8192 のほとんどを利用している．今回の実験において，ノード数 219 が求解限界となったのはこのアニーリング計算機の変数の制約が原因であり，今後，より大規模なアニーリング計算機が開発された際には，より大規模な遮断最適化問題を求解可能であると期待できる．

今回設計した単純化モデルおよび定式化を現実のネットワークに適用すること，また，定式化をより現実に即したものに改良していくことは今後の課題である．

参考文献

[1] Lucas, A.: Ising formulations of many NP problems, *Frontiers in Physics*, Vol. 2, p. 5 (2014).

[2] 平野遥，垣本修吾，米山一樹，山口純平：アニーリング計算を用いた AES の差分特性探索に向けて．信学技報，vol. 119，no. 474，ISEC2019-105，pp. 127-133，2020 年 3 月．

[3] Burges, C. J.: Factoring as optimization, *Microsoft Research* (2002).

[4] 清水俊也，伊豆哲也，篠原直行，盛合志帆，國廣昇：アニーリング計算による素因数分解について．SCIS2019，2019.

[5] 清水俊也，伊豆哲也，篠原直行，盛合志帆，國廣昇：アニーリング計算による素因数分解について（その 2）．SCIS2020，2020.

[6] 下山武司，大堀龍一，清水俊也，山口純平：アニーリングを用いた多変数多項式暗号解析．SCIS2019，2019.

[7] 山口純平，Mandal, A.，Montgomery, H.，Roy, A.，清水俊也，大堀龍一，下山武司：アニーリングを用いた格子問題の求解．SCIS2019，2019.

[8] 山口純平，清水俊也，古川和快：格子 enumeration に基づく SVP のハミルトニアンの構成と解読実験．SCIS2020，2020.

[9] 日本年金機構，不正アクセスによる情報流出事案に関する調査委員会：不正アクセスによる情報流出事案に関する調査結果報告．https://www.nenkin.go.jp/info/index.files/kuUK4cuR6MEN2.pdf.

[10] : Digital Annealer, Fujitsu. http://www.fujitsu.com/jp/digitalannealer/.

[11] : CMOS annealing machine, HITACHI. https://www.hitachi.co.jp/New/cnews/month/2019/02/0219.html.

[12] Oku, D., Terada, K., Hayashi, M., Yamaoka, M., Tanaka, S. and Togawa, N.: A fully-connected Ising model embedding method and its evaluation for CMOS annealing machines, *IEICE Transactions on Information and Systems*, Vol. 102, No. 9, pp. 1696–1706 (2019).

[13] Boros, E. and Hammer, P. L.: Pseudo-boolean optimization, *Discrete applied mathematics*, Vol. 123, No. 1-3, pp. 155–225 (2002).

[14] Rosenberg, I. G.: REDUCTION OF BIVALENT MAXIMIZATION TO THE QUADRATIC CASE. (1975).

[15] : 第 2 世代 Digital Annealer, Fujitsu. https://pr.fujitsu.com/jp/news/2018/12/21.html.

```
mv = [1220 1090 280 910 290 620 770 450 670 170 1660 640 320 580 120
970 160 1090 880 230 1420 220 660 730 540 670 450 1000 490 810]

W =
[[0 0 12 117 0 81 0 73 0 94 3851 0 0 0 0 0 0 0 0 0 1286 0 0 0 0 0 0 0 0 0]
[0 0 0 45 112 0 33 37 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 96 102 0 0 18 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 113 6 9 0 93 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 33 25 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 12 0 31 80 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 1 90 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 81 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 70 106 0 87 0 42 81 71 95 1856 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 54 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 108 0 0 66 63 91 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 112 0 58 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 19 113 44 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 85 0 75 117 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 108 60 4 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 88 0 0 4 15 34]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 41 107 0 5 0 18 70 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 57 11 45 54 0 94 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 83 52 106 112 86 4]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 80 37 0 64 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 52 112 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 85 32 106]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 115 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 75]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]]
```

図 **A·1**　$N = 30$ のクラスタ型グラフの資産価値 mv と通信量 w

付　　録

A.1　Appendix

小々節 4.3.2 で紹介したノード数 $N = 30$ のクラスタ型グラフにおいて，資産価値 mv と通信量 w を図 A·1 に示す．なお，配列 mv の第 i 成分はノード i の資産価値を，$i < j$ に対して 2 次配列 w の第 (i, j) 成分はノード i と j をつなぐ辺の通信量を表す（通信量 0 は辺が存在しないことを意味する）．