次世代分散ストレージのためのネットワーク構造と符号化方式の複合最適化

代表研究者　　西　山　大　樹　　東北大学　大学院情報科学研究科

1 研究調査の目的・意義

近年，情報通信サービスに利用されるコンテンツの大容量化に伴い，通信・収容効率に優れたストレージシステムの実現が期待されている．空間的にデータを分散・多重化する分散ストレージ技術は有効な解決策として期待されているが，サイバー攻撃が発生する環境においてさらなる性能向上が求められている．既存研究の多くはサイバー攻撃を検知する方法や検知できない場合でも防御する方法を提案することによってサービスの信頼性の向上を図ってきた．しかしながら，既存方式は下記の問題点を内包する．①未知の攻撃を検知・防御することは困難であると共に，様々な攻撃に適応できる分散ストレージ技術の設計は依然として未解決の重要な課題である．②ネットワーク構造や性能などの実環境を考慮した分散ストレージ技術が必要である．これらの問題を解決するためには，サイバー攻撃によって通信・計算機能やデータが失われた場合においてもサービス持続可能な分散ストレージシステムの実現が必要不可欠である．そこで本研究では，この目的を達成するための足掛かりとして，情報通信ネットワークの信頼性と符号化方式の信頼性を統合して評価するためのモデルを構築する．

本研究の遂行を通じて，分散ストレージシステムの高信頼化，ひいてはそれによって提供されている情報通信サービスの信頼性向上に貢献することができる．学問的には，本研究課題はネットワーク構造と符号化方式の複合最適化に向けた基礎理論を目指すものであり，情報通信工学，複雑ネットワーク理論，符号理論など応用情報工学の多岐にわたる分野を横断する．研究遂行を通して応用情報工学全体に対する大きな波及効果が期待できる．

2 国内外の研究動向

近年，クラウドストレージサービス高性能化の要求の高まりに伴い，高い信頼性を自動的に提供可能な分散ストレージシステムに注目が集まっている．国外では，カリフォルニア大学サンタクルーズ校 (UCSC) が，本分野の先駆けとして柔軟かつ拡張性に優れたオープンソース分散ストレージソフトウェアである Ceph を開発している[1]．Ceph を用いた分散ストレージシステムの実用化も進められており，Sage Well 社や Dream Host 社のクラウドストレージサービスの基盤技術として利用されている．他にも Amazon 社 Amazon S3[2]や Red Hat 社の GlusterFS[3]，OpenStack Swift[4]などの代表的な分散ストレージシステムが実用化されており，情報通信サービスを支える重要な技術として世界各地で研究開発が盛んに行われている．日本国内でも分散ストレージシステムの高度化・応用技術の研究開発が進められている．日本電信電話（株）は，従来と同等の容量効率・信頼性達成しつつ高い秘匿性を兼ね備える分散ストレージ技術を開発している[5]．スカパーJSAT(株)は地震や津波といった災害に対して有効な分散ストレージシステム SPlex3 を開発している[6]．富士通（株）は大規模な分散ストレージシステムにおける自律アクセス分散機能の研究開発を進めている．

以上の通り，数多くの分散ストレージシステム並びに関連技術が研究開発されてきているが，大規模なサイバー攻撃について十分考慮していない．ネットワーク構造と符号化方式がサービスの信頼性に与える影響を明らかにすることは，分散ストレージシステムの高信頼化にとって非常に重要な課題である．

3 想定環境と課題

3-1　無線データセンタネットワーク

3-1-1　無線化の必要性

従来，データセンタは大学や研究機関などでのデータ解析や情報通信サービスの提供といった限られた分野において利用されてきたが，近年では金融や行政，医療など幅広い分野の社会サービスにおいても利用されている．他方，データセンタで利用されるサーバの性能向上や広帯域化に伴うネットワーク機器の高性能化も著しい．これらデータセンタの規模拡大と高性能化に伴う消費電力増加は年々重大な問題となってきて

いる．実際，データセンタにおけるサーバ台数は年 1.2 倍の増加を続けており，それに伴う消費電力も増加を続け，2025 年には 4.6 兆 kWh の消費電力に達することが予想されている．これは，国内の総発電量の約半分を占める量であり，データセンタの消費電力削減は急務とされている．

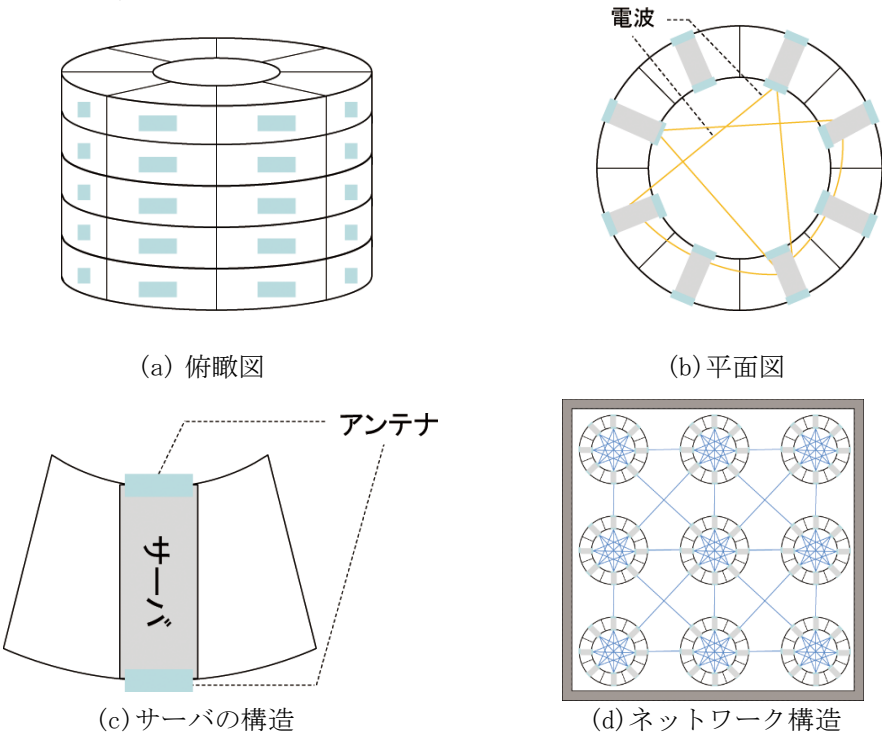
データセンタにおける電力消費の要因は，データセンタの冷却に要する電力（全体の 50%），各種スイッチなどのネットワーク機器が消費する電力（12%），データセンタのサーバが消費する電力（25%），その他種々の要因による消費電力の 4 つが挙げられる（13%）[7]．データセンタの冷却にかかる消費電力の増加は，データセンタで用いられる LAN（Local Area Network）ケーブルが通気性を阻害することによって発生している．また，データセンタのネットワークは冗長的な構造（例えば，Fat-tree topology）になっており，冗長なスイッチ類による消費電力の増加も問題である．

データセンタの冷却に要する電力とスイッチ類に要する消費電力問題は，サーバの無線化によって解決できる．無線化したサーバでデータセンタネットワークを構築することにより，LAN ケーブルを廃止することが可能であり，データセンタの通気性の大幅な向上とそれに伴う冷却の効率化が望まれる．また，各サーバに備え付ける無線アンテナは従来のスイッチ類に比べ大幅に小さい消費電力で稼働できる．例えば，60GHz 帯アンテナの消費電力は有線スイッチ類と比較して 0.0005～0.0017 倍程度である[8]．各サーバに無線アンテナを備え付けることを加味しても，ネットワーク全体の消費電力は大幅に削減可能である．

3-1-2　ネットワークアーキテクチャ

従来の優先接続されたデータセンタとは異なり，無線データセンタネットワークは各サーバが無線通信によって接続される．超広帯域かつ狭指向性の特徴を持つ 60GHz 帯無線アンテナを用いることにより，サーバ間の通信スループットを維持しつつ消費電力を低減できる[8]．

図 1 に本研究で着目する円筒型ラックを用いた無線データセンタネットワークを図示する．サーバラックは複数の薄い円筒状のラック（階層ラック）によって構成される（図 1 (a)）．各階層ラックには円上にサーバが配置される（図 1 (b)）．また，各サーバは内側と外側の両方に 60GHz 帯無線アンテナを持つ（図 1 (c)）．ラック内の通信においては，内側に備えられた無線アンテナを用いてマルチホップ通信を行うことで，目的サーバまでデータを伝送する．図 1 (d)はラックを複数配置した無線データセンタネットワークを図示している．各ラックは同様の大きさで，均一の間隔で配置されており，ラック間サーバの通信は外側に備えられた無線アンテナを用いて行われる．



(a) 俯瞰図　(b)平面図

(c)サーバの構造　(d)ネットワーク構造

図 1： 円筒状サーバラックを用いた無線データセンタネットワーク

この構造ではサーバラックの内部と外部で空間が分割されている．したがって，ラック間通信の電波は内部に伝搬せず，また同様にラック内通信の電波は外部へ伝搬しない．円筒型の構造を採用することで，電波干渉によるスループットの低下を抑えると共に，無線スペクトラムの有効利用が可能となる．また，ラック内のネットワーク（イントラネットワーク）とラック間のネットワーク（インターネットワーク）の両方がケイリーグラフの特徴持ち，その性質から高い連結性を達成できる．

3-2　消失訂正符号を用いた分散ストレージシステム

消失訂正符号を用いた分散ストレージシステムは，従来の RAID に基づく冗長化手法と比較して高信頼性かつ高速なデータ復旧が可能であり，また，複製による冗長化手法と比較して高い容量効率を達成可能であることが近年の研究で明らかになっている[9]．

図 2 に消失訂正符号を用いた分散ストレージシステムにおける基本的なデータ保存方法を示す．分散ストレージにデータが入力された時には，入力データを複数のシンボル（情報シンボル）に分割，分割したセグメントを基に消失訂正符号を用いて冗長シンボルを生成，それぞれのシンボルを独立したストレージサーバに保存する．入力データを読み取る時には，一定数のサーバからシンボルを収集し復号処理を行うことでデータを復元する．一方，サーバ故障時には，復元データを用いてシンボルを再生成することによって，故障したサーバに保存していたシンボルを復元する．以上の通り，消失訂正符号を用いた分散ストレージシステムではデータの信頼性を担保しつつ使用する記憶容量を低減することが可能である．

既存研究において，リードソロモン符号 [10]や再生成符号[11]など多くの消失訂正符号が提案されているが，本研究ではリードソロモン符号に着目する．リードソロモン符号を用いた分散ストレージシステムでは，分散配置するサーバ数を決定することでデータの冗長性（誤り訂正可能なシンボル数）を制御できる．データの冗長性を t，情報シンボル数（入力データの分割数）を k とする．このとき，必要となる冗長シンボル数は $2t$ であり，データ保存に必要となるストレージサーバ数 n は以下の式で与えられる．

$$n = k + 2t$$

但し，入力データ量 R が$R > k\,log_2\,n$の条件を満たす場合に限る．一方，使用可能なサーバ数が制限されている場合，保証可能な最大冗長性$\bar{t}$は以下の式で与えられる．

$$\bar{t} = \frac{n-k}{2}$$

また，冗長性を t，情報シンボル数（入力データの分割数）を k と設定したときに分散ストレージシステム全体で必要となる記憶容量 Vは以下の式で与えられる．

$$V = n \cdot \frac{R}{k} = \frac{(k+2t)R}{k}$$

複製による冗長化手法において必要となる記憶容量 V は$V = R \cdot t$で与えられるため，消失訂正符号を用いた冗長化手法は kを十分に大きな値に設定することで使用する記憶容量を低減することが可能である．

複製による冗長化手法はデータ復元時にサーバ間で通信する必要がない一方，消失訂正符号を用いた冗長化手法ではシンボル復元のために一つのサーバにシンボルを集約する必要がある．この時にネットワーク上を流れるトラヒック量 A は故障サーバ数$f(\leq t)$を用いて下記の式で与えられる．

$$A = \frac{R}{k}(n - f - 1)$$

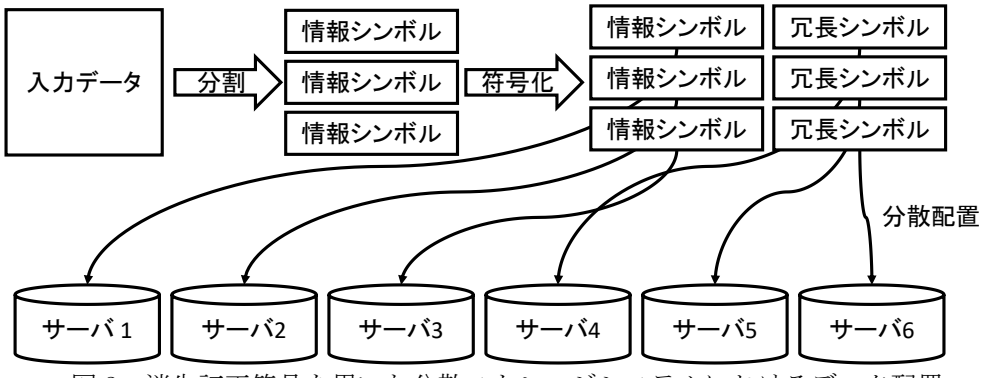


図 2: 消失訂正符号を用いた分散ストレージシステムにおけるデータ配置

4 分散ストレージシステムの性能評価モデル

3 章で説明したとおり，本研究では消失訂正符号を用いた分散ストレージシステムを無線データセンタネットワークで実行する環境を想定する．無線データセンタネットワークは各サーバがルータの役割も担うため，各サーバの故障は故障サーバのシンボル損失だけでなくネットワークの通信品質の低下やサーバの孤立によるシンボルの損失の原因となる．したがって，無線データセンタネットワークの冗長性と符号化の冗長性を統合してストレージサービスの性能（信頼性と復元コスト）を評価する必要がある．

4-1　無線データセンタネットワークにおける耐障害性

4-1-1　次数に基づく耐障害性の評価方法

本研究では，サイバー攻撃によってサーバの機能が停止する環境を想定する．また，サーバの機能停止確率はランダムだと仮定するとサーバの次数（通信可能なサーバ数）と独立して機能停止は発生する．この時，ネットワークの耐障害性（ネットワーク内で孤立するサーバが発生するために必要な機能停止サーバの割合）はネットワークの平均次数$\langle d\rangle$を用いて以下の式で求めることができる[12]．

$$P_{\mathrm{disr}} = 1 - \frac{1}{\langle d^2\rangle/\langle d\rangle - 1}$$

ネットワークの耐障害性と平均次数に関係性があるため，無線データセンタネットワークの構造を基にネットワークの平均次数の導出を行う必要がある．

4-1-2　無線データセンタネットワークの平均次数

想定する無線データセンタネットワークでは，各サーバの通信設定（放射角度・送信電力など）を同一に設定するため，基本的にサーバは同一の次数を持つ．しかしながら，ラックの最上部・最下部に配置されるサーバや壁面に配置されるサーバは隣接するサーバが少ないため他のサーバより低い次数を持つ．したがって，平均次数を向上するためには，全体のサーバに対する低次数サーバの割合を低減する必要がある．ラックの最上部・最下部に配置されるサーバの割合はラックを高くすること（階層ラック数を増加すること）で低減可能である．また，ラック数を増加することで壁面に配置されるサーバの割合を低くすることが可能である．

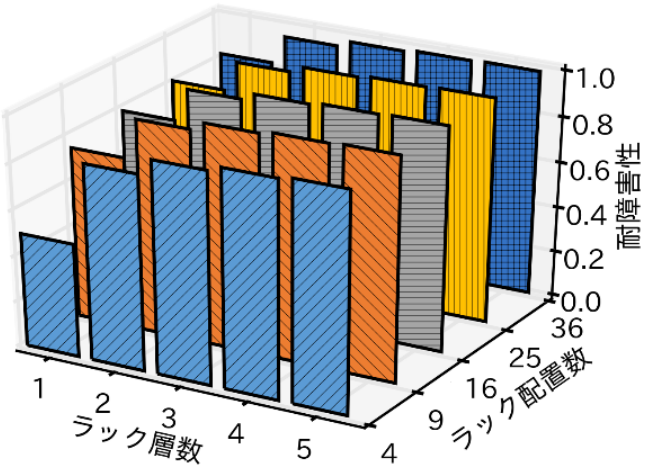


図 3: 無線データセンタの構造が耐障害性に与える影響

4-1-3　無線データセンタの構造と耐障害性の関係

ラック層数と配置ラック数が耐障害性に与える影響を数値解析によって評価した．ラックの直径を 1.21m，階層ラックの高さを 0.15m，各層に 8 サーバが収容されるラックを想定する．また，各サーバの電波到達距離は 1m でメインローブ半角は 25 度に設定した．この設定において無線データセンタネットワークの構造を変化させたときの耐障害性を図 3 に示す．この結果から，ラック層数とラック配置数が増加することで耐障害性を向上可能であることが分かる．また，耐障害性の増加割合に着目すると，耐障害性の向上にはラック

配置数よりラック層数の拡張が有効であることが分かる．

4-2　障害発生時の信頼性

ここでは，訂正符号を用いた分散ストレージシステムに対してサイバー攻撃が発生した際のデータ復元確率を求める．N台のサーバで構築される無線データセンタネットワークにおいて，冗長性tを保証するために消失訂正符号を用いてn台のサーバに入力データが分散配置される環境を想定する．さらに，サイバー攻撃の発生によってf台のサーバが機能停止になった時のデータの復元確率について考える．t台以下のデータ保存サーバが機能停止する場合にデータ復元が可能であるから，データ保存サーバが0からt台まで機能停止する確率をそれぞれ計算し，それらの総和を取ることでデータ復元確率が求められる．以上から，f台のサーバが機能停止になった時に任意のデータの復元が可能な確率は以下の式で求められる．

$$P_{\mathrm{rest}} = \frac{{}_nC_0 \cdot {}_{(N-n)}C_{(f-0)}}{{}_NC_f} + \frac{{}_nC_1 \cdot {}_{(N-n)}C_{(f-1)}}{{}_NC_f} + \cdots + \frac{{}_nC_t \cdot {}_{(N-n)}C_{(f-t)}}{{}_NC_f}$$

$$= \sum_{i=\max(0,f-(N-n))}^{t} \frac{{}_nC_i \cdot {}_{(N-n)}C_{(f-i)}}{{}_NC_f}$$

サーバの機能停止はサイバー攻撃による直接的な要因と隣接サーバの機能停止によって通信不可能になる間接的な要因に分類することができる．図 3 に示すように，一定数以上のサーバが機能停止することでネットワークの分断が発生し孤立したサーバは機能停止状態になる．従って，この両方の要因を加味した信頼性評価が必要である．

間接的な要因による機能停止サーバ数は無線データネットワークの次数分布を用いることで導出できる．サイバー攻撃発生前の次数分布をp_dとする．サイバー攻撃による機能停止は次数と関係なく発生するモデルを想定すると，サイバー攻撃発生後の生存サーバの次数分布p_d^Sはp_dと同等である．また，生存しているサーバの一部のリンクはサーバの機能停止によって取り除かれる．次数iの生存サーバのリンクが取り除かれる確率q_iは全てのiで同様に等しく，直接的な要因によって機能停止するサーバ数をf_{dir}と置くと$q_i = f_{\mathrm{dir}}/N$で表せる．従って，生存サーバのリンク除去後の次数分布は以下の式で与えられる[13]．

$$p'_d = \sum_{i=k} \binom{i}{k} p_i^S (q_i)^{i-k} (1-q_i)^k$$

さらに，リンク除去後の次数分布を基に孤立したサーバ（間接的な要因により機能停止したサーバ）の数f_{indir}は以下の式で求められる．

$$f_{\mathrm{indir}} = (N - f_{\mathrm{dir}}) \left(p'_0 + \sum_{d=1} p'_d \, (u_d)^d \right)$$

ここで，u_dは次数dのサーバと接続しているリンクが大規模クラスタに属していないサーバと接続している確率である．なお，u_dはモンテカルロ法によって導出する．

サイバー攻撃が発生した際の分散ストレージシステムの信頼性の評価を数値解析によって行った．図 3 と同等のラック，アンテナの設定を用いる．5 層のラックを 9 台配置するネットワークを想定する．この時，サーバ総数は 1440 台となる．冗長性を 2，入力データ分割数を 1 に設定し，各データを 5 台のサーバに分散配置する．サイバー攻撃の規模（直接的要因による機能停止サーバの割合）を 0.1～0.9 の間で変化させた時のデータ復元確率を評価する．図 4 に示すとおり， サイバー攻撃の規模が大きくなるにつれて，データ復元確率は低下する．規模が一定以上になると間接的な要因によってサーバが機能停止するため，データ復元確率は著しく低下する．図 5 はサイバー攻撃の規模を 0.3 に固定し，入力データ分割数を変化させた時のデータ復元確率とデータ配置に使用する記憶容量の関係である．なお，入力データは 10MB に設定した．入力データ分割数を大きくすることでより多くのサーバにデータを配置する必要があるため，データ復元確率は低下する．一方，入力データ分割数を大きく設定することで情報シンボルと冗長シンボルのデータ量を低下することが可能であるため，分割数を大きくすることで使用する記憶容量を低下することが可能である．以上の通り，入力データ分割数を設定する際にデータ復元確率と使用記憶容量にトレードオフの関係がある事が明らかになった．

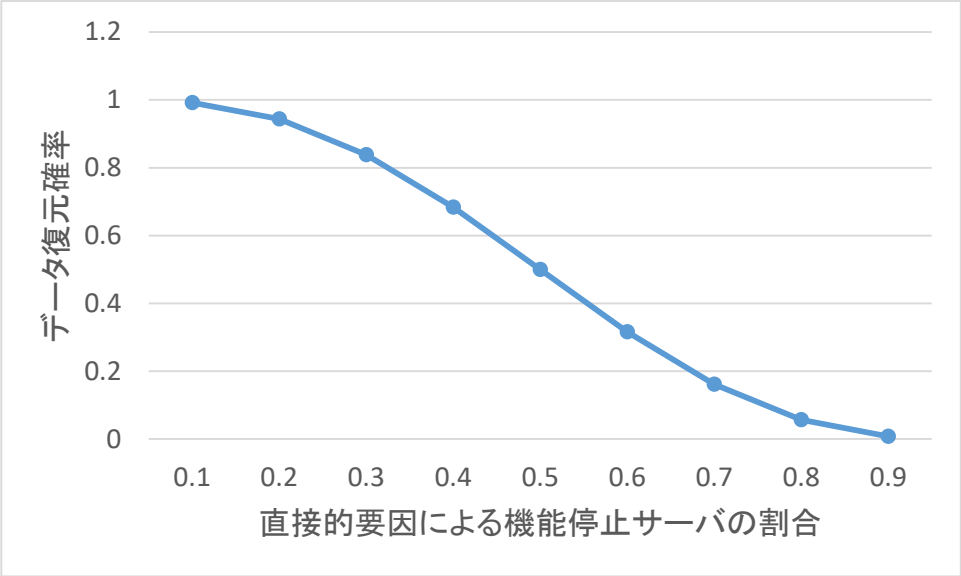


図 4: サイバー攻撃の規模がデータ復元確率に与える影響

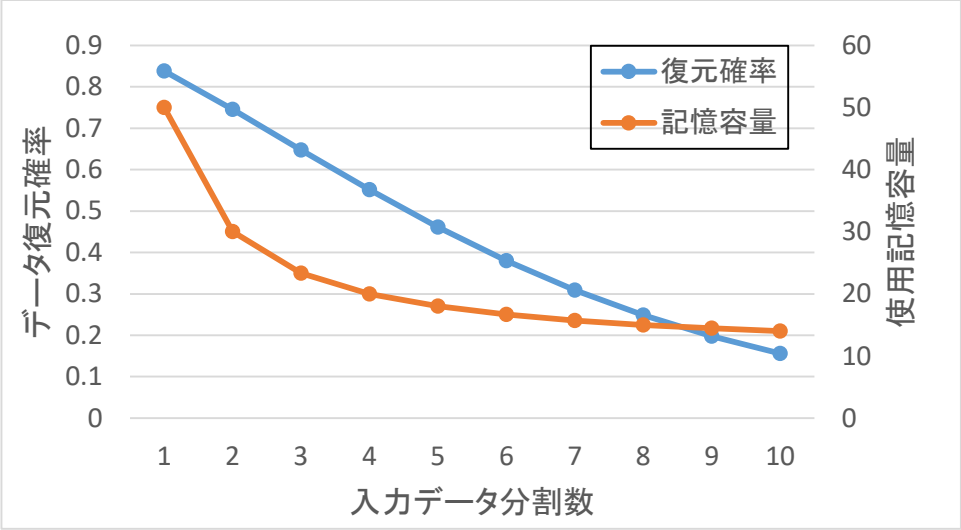


図 5:入力データ分割数におけるデータ復元確率と使用記憶容量のトレードオフ関係

4-3 障害発生時の復元コスト

無線データセンタネットワークはサーバ間のマルチホップ通信によってエンドツーエンドの情報伝達を実現するため，サーバが機能停止することによって平均ホップ数が増加し，ネットワーク上に流れるトラヒックの増加を促す．したがって，サイバー攻撃はデータの復元によるトラヒックの増加だけでなく平均ホップ数の増加に伴うトラヒックの増加を生む．そこで以降では，サイバー攻撃発生後のデータ復元に必要となるトラヒック量を評価するためのモデルを構築する．

まず，サイバー攻撃発生後にデータ復元のために保存シンボルを送信するサーバの数を導出する．t台よりも多くの保存サーバが機能停止した場合はデータの復元ができないため，t台以下の保存サーバが故障する場合にデータ復元は行われる．また，データ復元のために必要なシンボル数は$n-t$であり，受信サーバを除く他の生存サーバがそれぞれのシンボルを送信する．データ復元のためにシンボルを送信するサーバ数は常に$n-t-1$台となる．従って，サイバー攻撃発生後にある一つのデータを復元するために保存シンボルを送信するサーバの数S_{rest}は以下の式で与えられる．

$$S_{\mathrm{rest}} = \sum_{i=\max(0,f-(N-n))}^{t} \frac{{}_nC_i \cdot {}_{(N-n)}C_{(f-i)}}{{}_NC_f} \cdot (n-t-1)$$

上記の式から明らかなとおり，データ配置に利用するサーバ数および冗長性を増やすことによって，データ復元のためにシンボルを送信するサーバの期待値は増加する．また，機能停止するサーバが増加することでデータ復元を行わない確率が増えるため，データ復元のためにシンボルを送信するサーバの期待値は減少する．

次に，ある一つのデータを復元する時にネットワーク上に流れるトラヒック量の総和を導出する．送信サーバから受信サーバへマルチホップでシンボルが伝達するため，ネットワーク上に流れるトラヒック量の総和T_{rest}はネットワークの平均ホップ数$\langle H\rangle$を用いて以下の式で求められる．

$$T_{\mathrm{rest}} = S_{\mathrm{rest}} \cdot \frac{R}{k} \cdot \langle H\rangle$$

ここで，f台($f = f_{\mathrm{dir}} + f_{\mathrm{indir}}$)のサーバがサイバー攻撃によって機能停止した時のネットワークの平均ホップ数$\langle H'\rangle$はサイバー攻撃発生後のネットワークの平均次数$\langle d'\rangle$を用いることで近似的に導出できる[14]．

$$\langle H'\rangle = \frac{1}{\ln(\mu\langle d'\rangle)} \cdot \ln\left\{\left(N - f + \frac{\langle d'\rangle}{\mu\langle d'\rangle - 1} - 1\right) \cdot \left(\frac{\mu\langle d'\rangle - 1}{\langle d'\rangle}\right)\right\}$$

なお，μは近似係数であり，$\langle d'\rangle$は 4-2 章で導出したp'_dを用いて計算できる．上記の式から明らかなとおり，機能停止するサーバが増加することでホップ数は増加するためネットワーク上に流れるトラヒック量の総和は増加する．

5 研究調査成果，今後の課題

5-1　研究調査結果

本研究では，サイバー攻撃によって通信・計算機能やデータが失われた場合においても高品質のサービスを提供可能な分散ストレージシステムの実現を目標とし，ネットワーク構造と符号化方式の複合最適化を図るための数理モデルを構築した．まず，低消費電力を達成できる有望なデータセンタアーキテクチャとして期待されている無線データセンタネットワークの配置方法が耐障害性に与える影響を調査した．次に，無線データセンタネットワークにおけるサーバの機能停止要因を詳細に検討し，データ復元確率を精密に評価する数理モデルを提案した．また，入力データ分割数を変化させた時にデータ復元確率と使用記憶容量の間にトレードオフの関係があることを明らかにした．さらに，サイバー攻撃発生後データ復元をする時に必要となるネットワークコストを評価する数理モデルを提案すると共に，攻撃の規模とネットワークコストの定性的な関係を明らかにした．本研究では，情報通信ネットワークの信頼性と符号化方式の信頼性を統合して評価するための数理モデルを構築する事に成功した．本研究の成果は，次世代分散ストレージのためのネットワーク構造と符号化方式の複合最適化に必要となる基礎理論であり，分散ストレージシステムの高信頼化に向けた各種技術の礎となることが大いに期待できる．

5-2　今後の課題

無線データセンタネットワークにおける消失訂正符号を用いた分散ストレージシステムの性能を評価する事に成功したが，本研究には以下の課題が残っている．

- 本研究で想定した消失訂正符号はリードソロモン符号であるが，その他にも数多くの消失訂正符号がある．それらの消失訂正符号を用いた場合の評価モデルも必要である．
- それぞれの消失訂正符号には特徴がある．例えば，Minimum-Bandwidth Regenerating (MBR)符号はデータ復元に必要なトラヒック量が低く，Minimum-Storage Regenerating (MSR) 符号はストレージ利用効率が優れている[11]．したがって，与えられたネットワーク構造，ネットワーク性能，サーバ性能を基に最適な符号技術を選択する技術が必要となる．そのためにも，それぞれの符号方式に対応した評価モデルを構築する必要がある．
- ネットワーク性能としてデータ復元時に流れるトラヒック量（ネットワークコスト）を評価したが，他のネットワーク性能も評価する必要がある．例えば，無線データセンタネットワークの通信遅延を評価する数理モデルを構築することでデータ復元時間を評価可能になる．

【参考文献】

[1] Ceph, http://ceph.com/ (accessed 2016-4-1)
[2] Amazon, https://aws.amazon.com//s3/ (accessed 2016-4-1)
[3] GlusterFS, https://www.gluster.org/ (accessed 2016-4-1)
[4] OpenStack, http://docs.openstack.org/developer/swift/ (accessed 2016-4-1)
[5] 五十嵐 大, 露崎 浩太, 川原 祐人, "SHSS：オブジェクトストレージ向けの超高速秘密分散ライブラリ (情報通信システムセキュリティ)," 電子情報通信学会技術研究報告, vol. 115, no. 121, pp. 167-174, Jul. 2015.
[6] スカパーJSAT 株式会社, http://bcp.or.jp/pdf/gbs_101126/3_g-bcp101126.pdf (accessed 2016-4-1)
[7] T. Asami and S. Namiki, "Energy consumption targets for network systems," in proc. of European conference on Optical Communication, 2008, pp. 1-4.
[8] J-Y. Shin, E. G. Sirer, H. Weatherspoon, and D. Kirovski, "On the feasibility of completely wirelesss datacenters," IEEE/ACM Trans. on Networking, vol. 21, no. 5, pp. 1666-1679, Oct. 2013.
[9] H. Weatherspoon and J. Kubiatowicz, "Erasure Coding Vs. Replication: A Quantitative Comparison," in proc. of International Workshop on Peer-to-Peer Systems, 2002, pp. 328-338.
[10] V. Guruswami and M. Wootters, "Repairing Reed-Solomon Codes," arXiv:1509.04764v1, 15 Sep. 2015.
[11] A. G. Dimakis, et al., "Network Coding for Distributed Storage Systems," IEEE Transactions on Information Theory, vol. 56, no. 9, pp. 4539-4551, Sep. 2010.
[12] T. Tanizawa, et al., "Optimization of network robustness to waves of targeted and random attacks," Physical Review E, vol. 71, no. 4, Apr. 2005.
[13] B. Mitra, et al., "Analyzing the vulnerability of superpeer networks against attack," in proc. of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, Oct.-Nov. 2007, pp. 225–234.
[14] K. Suto, et al., "An Energy-Efficient and Delay-Aware Wireless Computing System for Industrial Wireless Sensor Networks," IEEE Access, vol. 3, pp. 1026-1035, Jul. 2015.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
無線データセンタにおける規模と耐障害性の関係の評価	電気関係学会東北支部連合大会	2015 年 8 月
広域分散ストレージシステムにおける効率的データ転送方式	電子情報通信学会 ソサイエティ大会	2013 年 9 月