修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院 情報システム学研究科 情報ネットワークシステム学専攻 博士前期課程		
氏　　名	中村　勇勝	学籍番号	1252024
論 文 題 目	閾値秘密分散保持されたコンテンツの高信頼・高効率配信法		

要　　旨

コンテンツを安全に保持するための閾値秘密分散法は，多重リンク障害に対する耐性が強い高信頼なコンテンツ配信にも応用することができる．複数の配信サーバに閾値秘密分散保持されているコンテンツを 1 つの配信先ノードに配信する際，高信頼なコンテンツ配信経路を算出するための発見的手法を既に提案している．しかし，閾値秘密分散保持されたコンテンツを各配信先ノードに個別に配信する方法では，ネットワークのリソース利用効率が低下する．

本論文では，閾値秘密分散保持されたコンテンツを，複数の配信先ノードに同時配信するコンテンツ配信法を提案する．複数の配信先ノードに同時配信することにより，ネットワーク符号化が適用でき，コンテンツ配信に必要なリンク帯域を削減できる．一方，ネットワーク符号化を適用した場合，リンク障害に起因する 1 つのピースの損失によって，配信先ノードにおいては，複数のピースのネットワーク復号化ができなくなる可能性があり，コンテンツ配信の信頼性は低下する．そこで，1 つのコンテンツを構成するピース群を複数のグループに分類し，ネットワーク符号化を同一グループに所属するピースに対してのみ適用する方法を提案する．ピース群を分類するグループ数を調節することにより，要求される信頼性を満足しつつ，リソース利用効率を最大化するコンテンツ配信の実現が期待できる．更に，実規模ネットワークにおける提案コンテンツ配信法の性能評価を行う目的から，欲張り法に基づき，提案コンテンツ配信法におけるコンテンツ配信経路を少ない計算量で算出する発見的手法を提案する．

提案コンテンツ配信法の有効性を示すために，NSF ネットワークと実規模のランダムネットワークを対象にして性能評価を行った．評価結果から，閾値秘密分散保持されたコンテンツを複数の配信先ノードに同時配信することにより，所要リンク帯域が減少し，効率的なコンテンツ配信を実現できることが判明した．また，コンテンツを構成するピース群を分類するグループ数の増加に伴い，リンク障害に対する信頼性は向上するが，リンク帯域利用効率は低下することが判明した．更に，提案コンテンツ配信法においては，配信経路の計算順序やピース群のグループ化の条件を変えることで，所要リンク帯域やピースの損失率が変化することが判明した．以上より，提案コンテンツ配信法において，ピース群のグループ数，配信経路の計算順序，ピース群のグループ化の条件を適切に設定することで，高信頼かつ高効率なコンテンツ配信を実現できる．

平成２５年度修士論文

【閾値秘密分散保持されたコンテンツの高信頼・高効率配信法】

大学院情報システム学研究科情報ネットワークシステム学専攻

学 籍 番 号： 1252024

氏　　名： 中村 勇勝

主任指導教員： 荻野 長生 客員准教授

指 導 教 員： 吉永 努 教授

指 導 教 員： 樫木 勘四郎 客員教授

提 出 年 月 日： 平成２６年１月２７日（月）

目次

1. 序論

ネットワークを介するコンピュータ間通信では，通信データの漏洩や盗聴あるいは障害発生による通信データの損失といった危険が伴う．コンテンツを安全に保持する方法として秘密分散法がある．秘密分散法では，コンテンツが複数のピースに分割され，1 つのコンテンツから生成されたピース群は複数の異なるサーバに分散保持される．例えば，(K,N)閾値秘密分散法は，1 つのコンテンツを N 個のピースに分割し，N 個のピースの内 K(K≦N)個以上のピースを集めないと元のコンテンツを復元できない技術である[1]．この様なコンテンツの安全保持を目的とした秘密分散法は，コンテンツの配信途中での盗聴を困難とする安全なコンテンツ配信，障害発生のリスクに強い高信頼なコンテンツ配信にも応用することが可能である[2-5].

(K,N)閾値秘密分散法の場合には，配信される N 個のピースの内，たとえ障害によって N－K 個のピースが損失したとしても，配信先ノードで元のコンテンツを復元することができる．しかし，各ピースの配信経路が同一リンクや同一ノードを通る場合，当該リンクや当該ノードの障害発生によって，多くのピースが配信先ノードまで転送できなくなり，配信先ノードでのコンテンツの復元が不可能になる確率が高くなる．よって，秘密分散法を利用したコンテンツ配信において，障害発生のリスクに強い配信を実現するためには，複数の配信経路が，できる限り同一リンクや同一ノードを通らないようにする必要がある．

閾値秘密分散法において N 個のピースを転送する際，各ピースが可能な限りリンク独立な配信経路を通ることで，多重リンク障害によって N－K＋1 個以上のピースが失われて，配信先ノードにおいて元のコンテンツが復元できなくなる確率を最小化することができる．各リンクの障害確率が与えられた時，配信先ノードで元のコンテンツが復元できなくなる確率を最小化する最適配信経路計算問題は，整数計画法モデルを用いて定式化することができる[6]．しかし，整数計画法モデルの直接解法には膨大な計算量が必要であり，整数計画法モデルの直接解法による配信経路計算法を実規模のネットワークに適用することはできない[7]．そこで，各ピースの配信経路を逐次的に算出することにより，複数の配信サーバに閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに配信するための高信頼なコンテンツ配信経路を少ない計算量で算出する方法を既に提案した[8]．しかし，コンテンツ配信要求が発生する度に，閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに個別に配信する方法では，ネットワークのリソース利用効率が低下する．

本研究では，(K,N)閾値秘密分散法によって複数の配信サーバに分散保持されたコンテンツを，複数の配信先ノードに同時配信する方法を提案する．閾値秘密分散保持されたコンテンツを同時に複数の配信先ノードに配信することにより，コンテンツ配信のタイミングが遅くなる恐れはあるが，ネットワーク符号化の適用によって，コンテンツ配信に必要なリンク帯域の有効利用が図れる．一方，ネットワーク符号化の適用によって，リンク障害に起因する 1 つのピースの損失によって，配信先ノードにおいて複数のピースのネットワーク復号化ができなくなる可能性がある．すなわち，ネットワーク符号化の適用によって，リソース利用

効率は向上するが，コンテンツ配信の信頼性は低下する．そこで，１つのコンテンツを構成するピース群を複数のグループに分類し，ネットワーク符号化を同一グループに所属するピースに対してのみ適用する方法を提案する[9]．ネットワーク符号化を適用するグループ数を調節することにより，要求される信頼性を満足しつつ，リソース利用効率を最大化するコンテンツ配信が実現できる．更に，提案コンテンツ配信法の性能評価を行う目的から，提案コンテンツ配信法におけるコンテンツ配信経路を少ない計算量で算出する方法を提案する．本研究では，NSF (National Science Foundation)ネットワークモデルと実用的な大規模ネットワークを対象にして具体的にコンテンツ配信経路の計算を行い，提案コンテンツ配信法の有効性を検証する．

以下，第 2 章では，本研究で提案するコンテンツ配信法に関して説明をする．第 3 章では，提案するコンテンツ配信法におけるコンテンツ配信経路計算法について説明する．第 4 章では，提案するコンテンツ配信法の性能評価を行い，提案法の有効性を示す．第 5 章では，本研究の結論を述べる．

2. コンテンツの高信頼・高効率配信法

本章では，既存研究である複数の配信サーバに閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに配信する高信頼なコンテンツ配信法に関して説明する．また，本手法における課題について説明し，課題を解決するために本研究で提案する高信頼・高効率コンテンツ配信法について説明する．

2.1 (K,N)閾値秘密分散保持されたコンテンツの配信

図 2.1 に示すように,(K,N)閾値秘密分散法は,1 つのコンテンツを N 個のピースに分割し，分割した N 個のピースから K 個以上のピースを集めると元のコンテンツが復元できる技術である．これにより，ピースを複数の配信サーバで秘密分散保持することで安全なコンテンツ保持が実現できる．また，閾値秘密分散保持されたコンテンツの配信を行った場合，配信される N 個のピースの内，N－K 個のピースが何らかの障害によって損失したとしても，K 個以上のピースさえ配信先ノードで集めることができれば，元のコンテンツを復元することが可能となる．つまり，閾値秘密分散法を応用することで，信頼性の高いコンテンツ配信を実現することが可能である．

図 2.1：(K,N)閾値秘密分散法の概要

しかし，複数の配信サーバに閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに転送する際，コンテンツを構成する各ピースの配信経路が同一のリンクや同一のノードを通ると,図 2.2 のようなリンクやノードに障害が発生した場合,多数のピースが損失してしまう．そして，リンク障害やノード障害により，配信先ノードで元のコンテンツを復元できなくなる確率が高くなる．従って，リンク障害に対して信頼性の高いコンテンツ配信法を実現する

ためには，互いに重複しないリンク独立な配信経路を計算する必要がある．しかし，通常のバックボーンネットワークでは，配信サーバから配信先ノードまでのピース分のリンク独立な経路は存在しない．そのため，各ピースが可能な限りリンク独立な経路を通ることで，元のコンテンツを復元できなくなる確率を最小化する必要がある．そこで既存研究では，複数の配信サーバに閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに配信するための高信頼なコンテンツ配信経路の算出法を提案した．

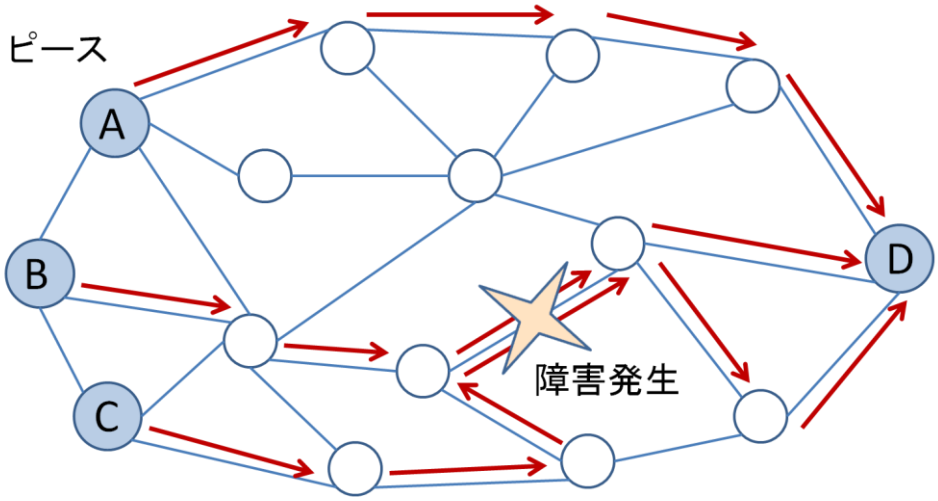

図 2.2：コンテンツ配信経路問題

2.2　複数配信先ノードに対する同時配信

複数の配信サーバに閾値秘密分散保持されたコンテンツを配信する際，コンテンツの配信を要求する複数の配信先ノードに同一コンテンツを個別に配信する方法では，ネットワークのリソース利用効率が低下する．そこで，閾値秘密分散保持されたコンテンツを複数の配信先ノードに同時配信することで，コンテンツ配信のタイミングが遅くなる恐れはあるが，効率的なコンテンツ配信を実現することを考える．つまり，本研究では，閾値秘密分散保持されたコンテンツを複数の配信先ノードに同時配信することで，十分な信頼性を満足しつつ，リソース利用効率を向上させることができるコンテンツ配信法を提案する．

図 2.3 に示すように，複数の配信サーバに閾値秘密分散保持されているコンテンツを構成する各ピースを中継ノードで複製して複数の配信先ノードに転送することで，各ピースのマルチキャスト配信を実現できる．また，閾値秘密分散保持されているコンテンツを構成する各ピースを複数の配信先ノードに同時配信する際，中継ノードでネットワーク符号化を適用することで，異なる配信先ノードに向かう複数の異なるピースを 1 つのピースに符号化して，複数の配信先ノードに同時配信することが可能となる．すなわち，閾値秘密分散保持されたコンテンツを複数の配信先ノードに同時配信することで，マルチキャスト配信の効果とネットワーク符号化の効果によって，ネットワークのリソース利用の効率化を図ることができる．

例えば，配信サーバ 1 に保持されているピース A と配信サーバ 2 に保持されているピース

B は，中継ノードでネットワーク符号化の効果により，1 つのピースとしてまとめられ配信先ノード 1 と配信先ノード d に配信される．また，配信サーバ N に保持されているピース C は，マルチキャスト転送の効果により，中継ノードで複製されて配信先ノード 1 と配信先ノード d に配信される．

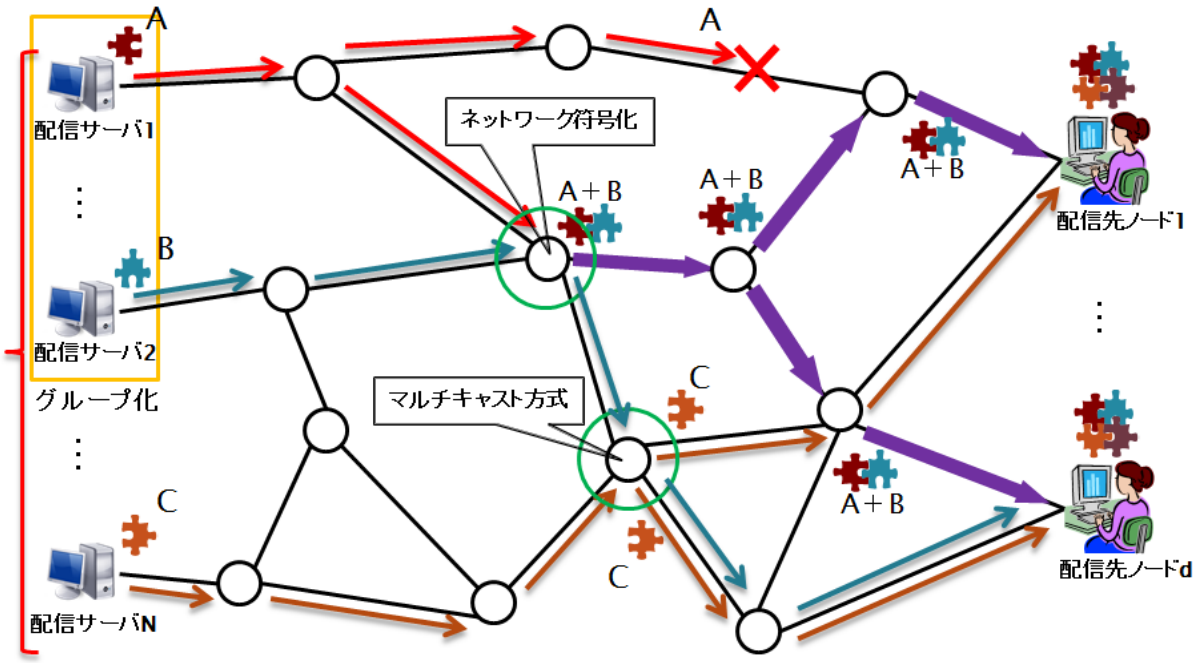

図 2.3：同時配信によるネットワーク符号化の適用

2.3　ピース群のグループ化

閾値秘密分散保持されたコンテンツを複数の配信先ノードに同時配信すれば，ネットワーク符号化の適用によって，リソース利用効率が向上するが，リンク障害に起因する 1 つのピースの損失によって，配信先ノードにおいて複数のピースのネットワーク復号化ができなくなり，結局，配信先ノードで元のコンテンツを復元できない状況を引き起こす恐れがある．

図 2.3 のように，配信サーバにそれぞれ A，B，C というピースが分散保持されているとする．中継ノードによってピース A とピース B がネットワーク符号化により 1 つのピースとして配信先ノード 1 に配信される．この時，ピース A が障害によって途中経路で損失してしまうとする．ネットワーク符号化されたピース A とピース B が配信先ノード 1 に配信されたとしても，ピース A が配信先ノード 1 に配信されなければ，ピース A とピース B 共にネットワーク復号化ができなくなる．すなわち，1 つのピースの損失によって，配信先ノードにおいて 2 つのピースのネットワーク復号化ができなくなる．

つまり，ネットワーク符号化は，リソース利用効率を向上させることが可能だが，コンテンツ配信の信頼性を低下させてしまう可能性がある．そのため，本研究におけるコンテンツ配信法として，複数の配信サーバに閾値秘密分散保持されているコンテンツを構成するピー

ス群をあらかじめ複数のグループに分割し，同一グループに属するピースに対してのみネットワーク符号化を適用する方法を提案する．

ピース群のグループ化により，あるピースがリンク障害によって損失したとしても，配信先ノードでネットワーク復号化できなくなる可能性のあるピースは，損失したピースと同一グループに属するピースのみに制限できる．グループ数を多くすると，ネットワーク符号化によるリソース利用効率向上の効果は減少するが，多重リンク障害によって元のコンテンツを復元できなくなる配信先ノード数の期待値をより小さくできる．すなわち，グループ数を調節することにより，リンク障害に対する信頼性とリソース利用効率のトレードオフを制御することが可能なコンテンツ配信を実現できる．

図 2.4 に，ネットワーク符号化の適用によって，リンク帯域が複数の配信経路により共用される様子を示す．なお，横軸は D 個の配信先ノードを示し，縦軸は N 本の配信経路を示している．N 本の配信経路に対応する N 個のピース群は，n_1 個のピースから構成されるグループ 1 と n_2 個のピースから構成されるグループ 2 に分割されている．図 2.4 において，配信先ノード 2 に至る配信経路 1 と配信先ノード 3 に至る配信経路 1 は，マルチキャスト配信によって互いにリンク帯域を共用できる．また，配信先ノード 1 に至る配信経路 2 と配信先ノード 2 に至る配信経路 2 と配信先ノード 3 に至る配信経路 2 は，マルチキャスト配信によって互いにリンク帯域を共用できる．更に，配信先ノード 2 に至る配信経路 n_1+2 と配信先ノード D に至る配信経路 n_1+2 とは，マルチキャスト配信によって互いにリンク帯域を共用できる．最後に，同じグループ 2 に所属する配信先ノード 1 に至る配信経路 n_1+n_2 と配信先ノード 2 に至る配信経路 n_1+1 は，ネットワーク符号化によって互いにリンク帯域を共用できる．

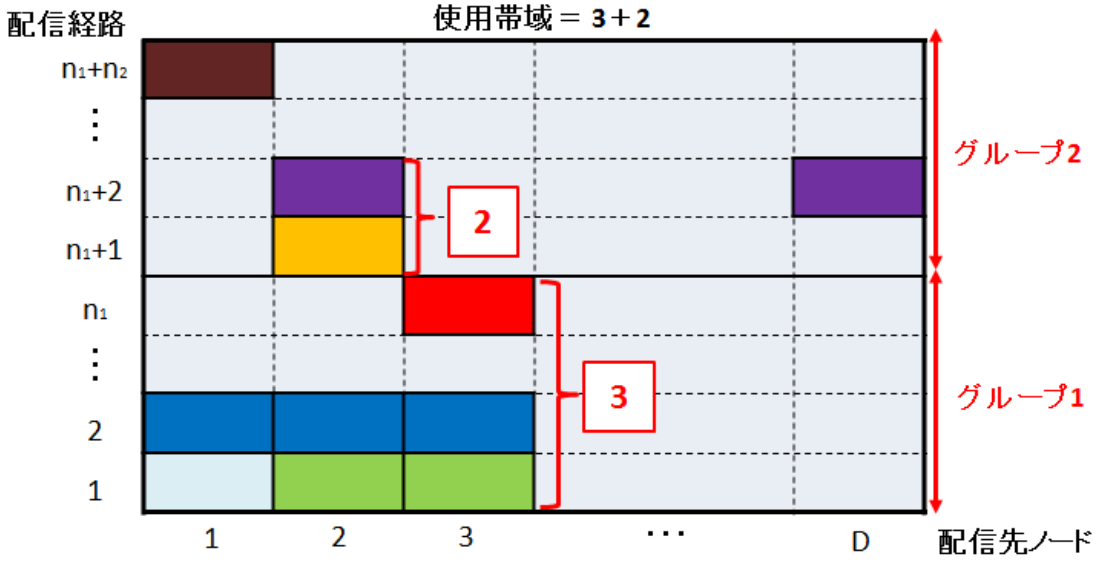

図 2.4：ネットワーク符号化によるリンク帯域容量の共用

以上より，リンク使用帯域は，グループ 1 に所属して各配信先ノードに至る配信経路の中で最大である配信先ノード 3 に至る配信経路数 3 とグループ 2 に所属して各配信先ノードに

至る配信経路数の中で最大である配信先ノード2に至る配信経路数2とを加算した値である5となる．これに対して，ピース群のグループ化を行わない場合には，配信先ノード 1 に至る配信経路 n_1+n_2 と配信先ノード 2 に至る配信経路 n_1+1 に加えて，配信先ノード 3 に至る配信経路 n_1 も，ネットワーク符号化によって互いにリンク帯域を共用でき，リンク使用帯域は4となる．しかし，図 2.4 に示したリンクに障害が発生した場合，ピース群のグループ化を行わない時は，配信先ノード D において全てのピースのネットワーク復号化ができなくなる可能性があるのに対して，グループ化を行う時は，配信先ノード D においてネットワーク復号化ができなくなる可能性があるピースは，グループ 2 に所属するピースに限定される．同一グループに所属するピースに対してのみネットワーク符号化を適用することにより，多少リンク帯域容量が増加してしまうが複数の配信サーバで閾値秘密分散保持されているコンテンツを複数の配信先ノードまでネットワークを介して同時転送する際，リンク帯域の有効利用を図りつつ，多重リンク障害によって元のコンテンツを復元できなくなる配信先ノード数の期待値を最小化する高信頼なコンテンツ配信が可能となる．

3. 提案コンテンツ配信法における配信経路計算法

提案コンテンツ配信法の性能評価を行うためには,複数の配信サーバで閾値秘密分散保持されているコンテンツを構成する各ピースの配信経路を具体的に算出する必要がある．本章では，提案コンテンツ配信法における配信経路計算問題で用いられる整数計画法モデルの定式化について説明し，整数計画法モデルを用いたコンテンツ配信経路計算の求解に関する問題点を解決する目的で提案するコンテンツ配信経路の発見的計算アルゴリズムについて説明する．

3.1 配信経路計算問題の定式化

本節では，整数計画法モデルを用いて，本研究で対象とするコンテンツ配信経路計算問題を厳密に定式化する．S 個の配信サーバに(K,N)閾値分散保持されたコンテンツを D 個の配信先ノードに同時配信する場合を考える．(Step1)から(Step2)の流れで，多重リンク障害によって N 個のピースのうち N－K＋1 個以上のピースが損失し,元のコンテンツを復元できなくなる配信先ノード数の期待値を最小化する N×D 本の配信経路を求める整数計画法モデルを求める．

(Step1)

配信サーバ群から配信先ノード d に至るリンク独立な経路の最大数が m である場合は，配信サーバ群から配信先ノード d に至る N 本の配信経路全てが，ある m 本のリンク組に含まれるいずれかのリンクを必ず通過すると考えられる．また, D 個の各配信先ノード d について，それぞれリンク独立な経路の最大数 m の中から，最小値を M とする．この時，リンク独立な経路の最大数が M であるような配信先ノード d に至る N 本の配信経路は，ある M 本のリンク組に含まれるいずれかのリンクを通過することになる．

このような N 本の配信経路をリンク容量は考慮せず,できるだけ均等(整数単位で最も均等)に M 本のリンクに分配することを考える．N 本の配信経路を M 本のリンクに均等に配分する際，N－K＋1 本の配信経路を含む最小のリンク数 F が算出される．つまり，i(=1~M)番目のリンクには式(1)で与えられる h_i 本の配信経路が配分される．

$$\begin{cases} h_i = [N/M] + 1 \ , \ 1 \le i \le H \\ h_i = [N/M] \ , \ H + 1 \le i \le M \end{cases} \qquad (1)$$

(ただし，[x]は，x 以下の最大整数)

また，H は式(2)で与えられる．

$$\mathrm{H} = \mathrm{N} - [\mathrm{N}/\mathrm{M}] \times \mathrm{M} \qquad (2)$$

リンク数 F は, 配分される配信経路数の総和が N－K＋1 本以上となる最小リンク数として, 式(3)で与えられる.

$$\mathrm{F} \leftarrow \arg\min_{f}\left(\left(\sum_{i=1}^{f} h_i \geq N-K+1\right)=true\right) \qquad (3)$$

この時，M 本のリンク中 F 本のリンクに障害が発生すると，リンク独立な経路の最大数が M であるような配信先ノードでは，各ピースを転送するための N 本の配信経路のうち，必ず N－K＋1 本以上の配信経路が障害となる．リンク容量の制約によって，F 本よりも少ないリンク障害によって，ある配信先ノードに至る N－K＋1 本以上の配信経路が障害になる可能性もあるが，リンク容量の制約が全く存在しない場合でも，F 重リンク障害によって，N－K＋1 本以上の配信経路が必ず障害になる．つまり，ネットワーク符号化が全く実行されない場合でも，F 重リンク障害によって，N－K＋1 個以上のピースが損失となり，ある配信先ノードでは元のコンテンツを復元できなくなる．

各リンクの障害確率は十分小さいと仮定し，いずれかの配信先ノードで必ず元のコンテンツが復元できなくなる F 重リンク障害以下の多重リンク障害のみを考慮する．つまり，F 重リンク障害以下の多重リンク障害が発生した時，元のコンテンツを復元できなくなる配信先ノード数の期待値が最小となるような配信経路の算出を考える．

(Step2)

F 重リンク障害以下の多重リンク障害によって, D 個の配信先ノードに対して元のコンテンツを復元できない配信先ノード数の期待値を最小化するような N×D 本の配信経路を算出する．この時，N 個のピースを G 個のグループに分割し，各中継ノードは同一グループに属して配信先ノードが異なるピースのみに対し，ネットワーク符号化を適用する．そして，あるピースが損失した場合は，ネットワーク符号化が適用される当該ピースと同一グループに属するピースも全て損失すると考える．コンテンツ配信経路計算問題は，以下の様に整数計画法モデルを用いて定式化できる．

最初に，図 3.1 のようにネットワークトポロジを変形する．すなわち，新たに擬似発ノード vs を設けて，各配信サーバ s(vlink)へ仮想リンク vlink を接続する．各仮想リンクの障害確率はゼロとし, 各仮想リンクの容量は, 接続している配信サーバが保有しているピース数 $C_{s(vlink)}$ に設定する．本ネットワーク変形により，各配信サーバが保持するピース数を考慮して，コンテンツ配信経路を計算できる．

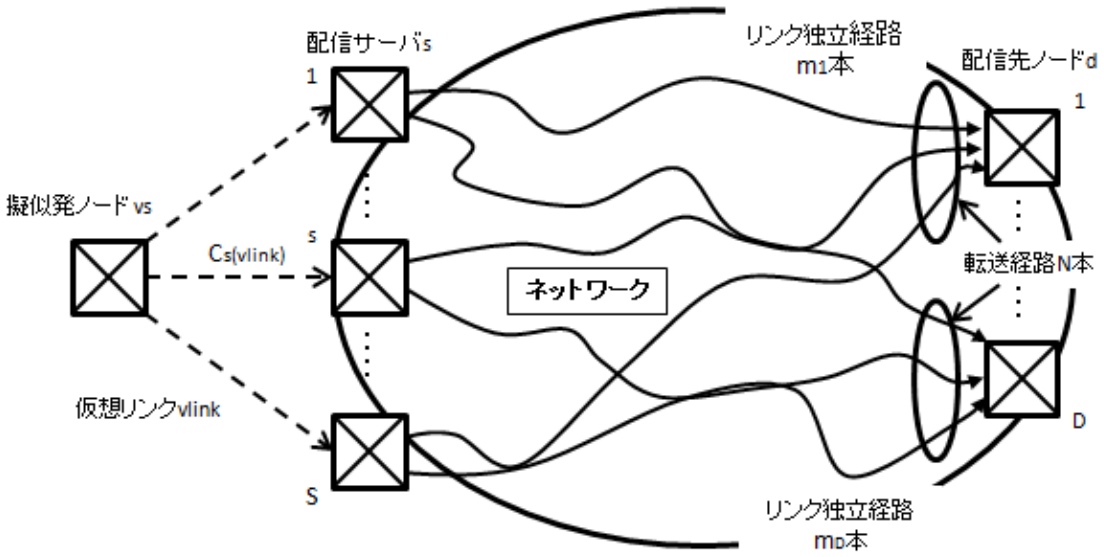

図 3.1：ネットワークトポロジの変形

整数計画法モデルにおける定数及び集合は，以下のように定義される．

- node：ネットワークを構成するノード
- Node：擬似発ノードを除くノード node の集合
- d：配信先ノード
- link：ネットワークを構成するリンク
- Link：仮想リンクを含むリンク link の集合
- vs：擬似発ノード
- vlink：仮想リンク
- VLink：仮想リンクの集合
- s(vlink)：仮想リンク vlink が接続する配信サーバ
- $C_{s(vlink)}$：配信サーバ s(vlink)が保有しているピース数
- C_{link}：仮想リンクを除く各リンク link の容量
- IN_{node}：ノード node を終点とするリンクの集合
- OUT_{node}：ノード node を始点とするリンクの集合
- xlink：リンク link を通過するリンク独立経路の本数を表す整数変数
- m：リンク独立な経路の本数
- Dest：配信先ノードの集合
- FLink：仮想リンクを含まない F 本以下のリンク組合せの集合
- $FLink_f$：FLink 内の f 番目の組合せに含まれるリンクの集合
- P_{link}：予め与えられているリンク link の障害確率
- GPC_g：グループ g(1~G)に属する配信経路の集合
- ng：グループ g(1~G)に属する配信経路数

整数計画法モデルにおける変数は，以下のように定義される．

- $X_{link(d,n)}$：配信先ノード d(1~D)に至る n(1~N)番目の配信経路が，リンク link を通過する時「1」，そうでない時「0」であるバイナリ変数
- $C_{link(g)}$：グループ g に属する配信経路による仮想リンクを除くリンク link の使用帯域を表す整数変数
- $Y_{f(d,g)}$：リンク組合せ $FLink_f$ の多重リンク障害によって，配信先ノード d(1~D)において，グループ g(1~G)に属するピースをネットワーク復号できない時「1」，復号できる時「0」であるバイナリ変数
- $Z_{f(d)}$：リンク組合せ $FLink_f$ の多重リンク障害によって，配信先ノード d(1~D)において，N－K＋1 個以上のピースをネットワーク復号できず，元のコンテンツを復元できない時「1」，復元できる時「0」であるバイナリ変数

更に，整数計画法モデルにおける制約式は，式(4)～(11)で与えられる．式(4)は，各 N 本の配信経路が，擬似発ノードから出る仮想リンクの中の 1 本だけを通る．つまり，N 本の配信経路は擬似発ノードから出る仮想リンクのいずれかを通るという経路保存則である．

$$\sum_{vlink \in VLink} X_{vlink}(d,n) = 1 \quad , \quad \forall d = 1 \sim D \ , \ \forall n = 1 \sim N \qquad (4)$$

式(5)は，全ての配信経路は配信先ノードに入るリンクのいずれかを 1 回だけ通過し，配信先ノードから出るリンクを通過することはないという経路保存則である．

$$\sum_{link \in INd} X_{link}(d,n) = 1 \ , \quad \sum_{link \in OUTd} X_{link}(d,n) = 0 \ , \ \forall d = 1 \sim D \ , \ \forall n = 1 \sim N \qquad (5)$$

式(6)は，全ての配信経路が擬似発ノード及び配信先ノード d 以外の中継ノードを始点とするリンク及び終点とするリンクを 1 回だけ通過するか，どちらも通過しないという経路保存則である．

$$\sum_{link \in INnode} X_{link}(d,n) = \sum_{link \in OUTnode} X_{link}(d,n) \leq 1 \ ,$$
$$\forall node \neq d \in Node \ , \ \forall d = 1 \sim D \ , \ \forall n = 1 \sim N \qquad (6)$$

また，仮想リンク vlink の容量条件が式(7)で与えられる．これは，擬似発ノード vs と各配信サーバ s(vlink)とを結ぶ仮想リンク vlink を通過する配信経路の本数であり，配信サーバ s(vlink)から配信されるピース数は，当該配信サーバ s(vlink)が保持しているピース数 $C_{s(vlink)}$ をこえないという条件となる．

$$\sum_{n=1}^{N} X_{vlink}(d,n) \le C_{s(vlink)}\,,\ \forall vlink \in VLink\ ,\ \forall d = 1\sim D \qquad (7)$$

式(8)，(9)は，ネットワーク符号化を前提としたリンク容量の制約である．各グループに属するピースによる各リンクの使用帯域は，当該リンクを通過して各配信先ノードに至る配信経路数のうちの最大数となり，各リンクの使用帯域はリンク容量以下でなければならない．

$$\sum_{n\in GPCg}^{N} X_{link}(d,n) \le C_{link}(g)\,,\ \forall link \in Link - VLink\ ,\ \forall d = 1\sim D \qquad (8)$$

$$\sum_{g=1}^{G} C_{link}(g) \le C_{link}\,,\ \forall link \in Link - VLink \qquad (9)$$

式(10)は，各々の多重リンク障害によって，各配信先ノードにおけるピースのネットワーク復号ができない条件である．

$$Y_f(d,g) \ge X_{link}(d,n)\,,$$
$$\forall n \in GPCg\ ,\forall link \in FLinkf\ ,\forall g = 1\sim G\ ,\forall FLinkf \in FLink\ ,\forall d = 1\sim D \qquad (10)$$

式(11)は，各々の多重リンク障害によって，各配信先ノードにおける元のコンテンツの復元ができない条件である．なお，符号 A は十分大きな値を持つ正定数である．

$$-\mathrm{A}\times\left(1 - Z_f(\mathrm{d})\right) + 1 \le \sum_{g=1}^{G} n_g Y_f(d,g) - (N-K) \le A \times Z_f(d)\ ,$$
$$\forall FLinkf \in FLink, \forall d = 1\sim D \qquad (11)$$

本整数計画法モデルの目的は，F 重リンク障害以下の多重リンク障害によって N 個のピースのうち，N－K＋1 個以上のピースが損失し，元のコンテンツを復元できなくなる配信先ノード数の期待値を最小化することにある．最小化すべき目的関数は，次式(12)で与えられ，本整数計画法モデルを解法することによって得られる $X_{link(d,n)}$の値から，各配信先ノード d に至る N 本の配信経路が計算される．

$$\mathrm{Obj} = \sum_{FLinkf\in FLink}\left(\prod_{link\in FLinkf} P_{link} \times \sum_{d=1}^{D} Z_f(d)\right) \qquad (12)$$

3.2　発見的コンテンツ配信経路計算法の提案

本節では，整数計画法モデルの直接解法によって，図 3.2 に示すようなコンテンツ配信経路計算問題を求解する際の問題点について説明する．そして，本研究で提案する発見的コンテンツ配信経路計算法のアルゴリズムについて説明する．

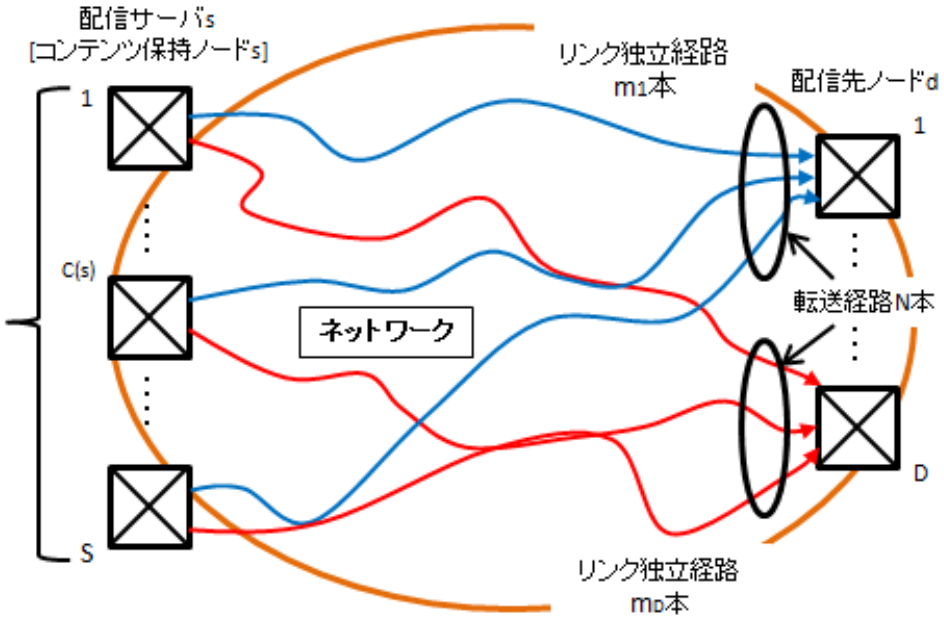

図 3.2：コンテンツ配信経路問題

3.2.1　整数計画法モデルの問題点

各リンクの障害確率が与えられた時，元のコンテンツを復元できない配信先ノード数の期待値を最小化する最適配信経路計算問題は，整数計画法モデルを用いて定式化することができる．定式化した整数計画法モデルを直接解法することで，厳密に最適な配信経路を算出することが可能となる．しかし，整数計画法モデルの解法には膨大な計算量が必要であり，小規模ネットワークで適用できたとしても，実用規模のネットワークに適用することは，計算時間の観点から困難である．このことから，実用的なネットワークに対しても高速に計算を行うことが可能な発見的なコンテンツ配信経路計算法が要求される．

3.2.2　発見的コンテンツ配信経路計算法のアルゴリズム

本研究で提案する発見的コンテンツ配信経路計算法では，図 3.3 に示すようなアルゴリズムで配信経路の算出を行う．配信経路算出に関しては，欲張り法の考え方に基づき，各配信先ノードに対して，ピース N 個分の配信経路をダイクストラ法の適用により 1 本ずつ逐次的に計算する．つまり，逐次的な配信経路計算の各段階において，常に N－K＋1 個以上のピース

が損失する確率の増加分(所要リンク帯域の増加分)を最小化するように，更新したリンクコストの下で最小コスト経路を計算する．同様な計算処理を D 個の配信先ノードに対して繰り返し行う．本配信経路計算法では，ダイクストラ法を N×D 回繰り返し実行するのみなので，コンテンツ配信経路を少ない計算量で高速に計算することが可能となる．

また，ピースの損失が起きた場合，当該ピースと同一グループに所属する全てのピースが損失したと見なすことで，各中継ノードにおいてネットワーク符号化されるピースの実際の組合せを考慮することなく，信頼性に関して安全側のコンテンツ配信経路を容易に計算できる．以上から，本コンテンツ配信経路計算法を適用することで，要求される信頼性を満足しつつ効率性を最大化するコンテンツ配信経路の計算を高速に行うことが可能となる．

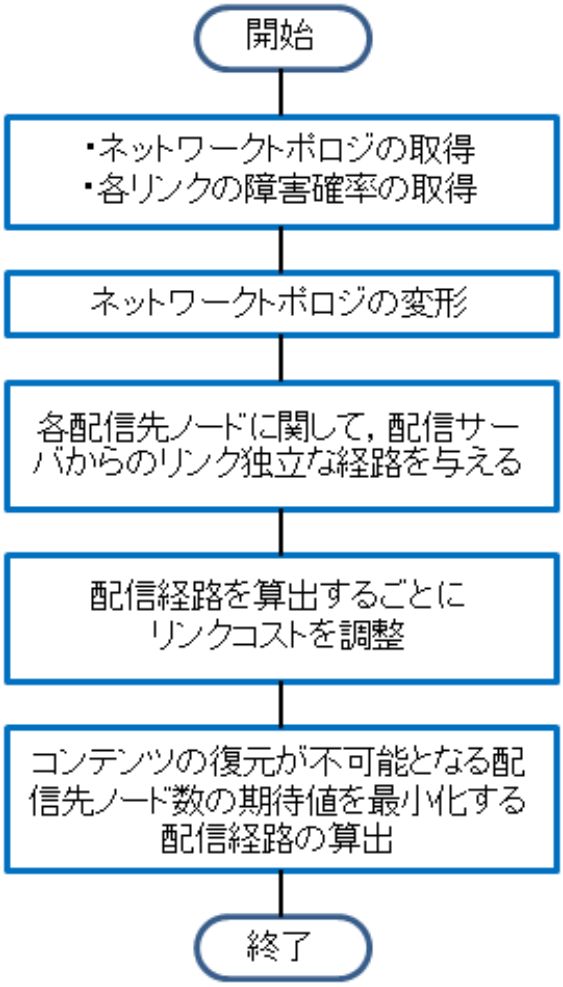

図 3.3：発見的コンテンツ配信経路計算のアルゴリズム

3.3　コンテンツ配信経路の計算手順

コンテンツ配信経路の計算手順について，図 3.4 に示す．また，コンテンツ配信経路の計算は，以下の(Step1)から(Step4)の段階に分かれて処理される．

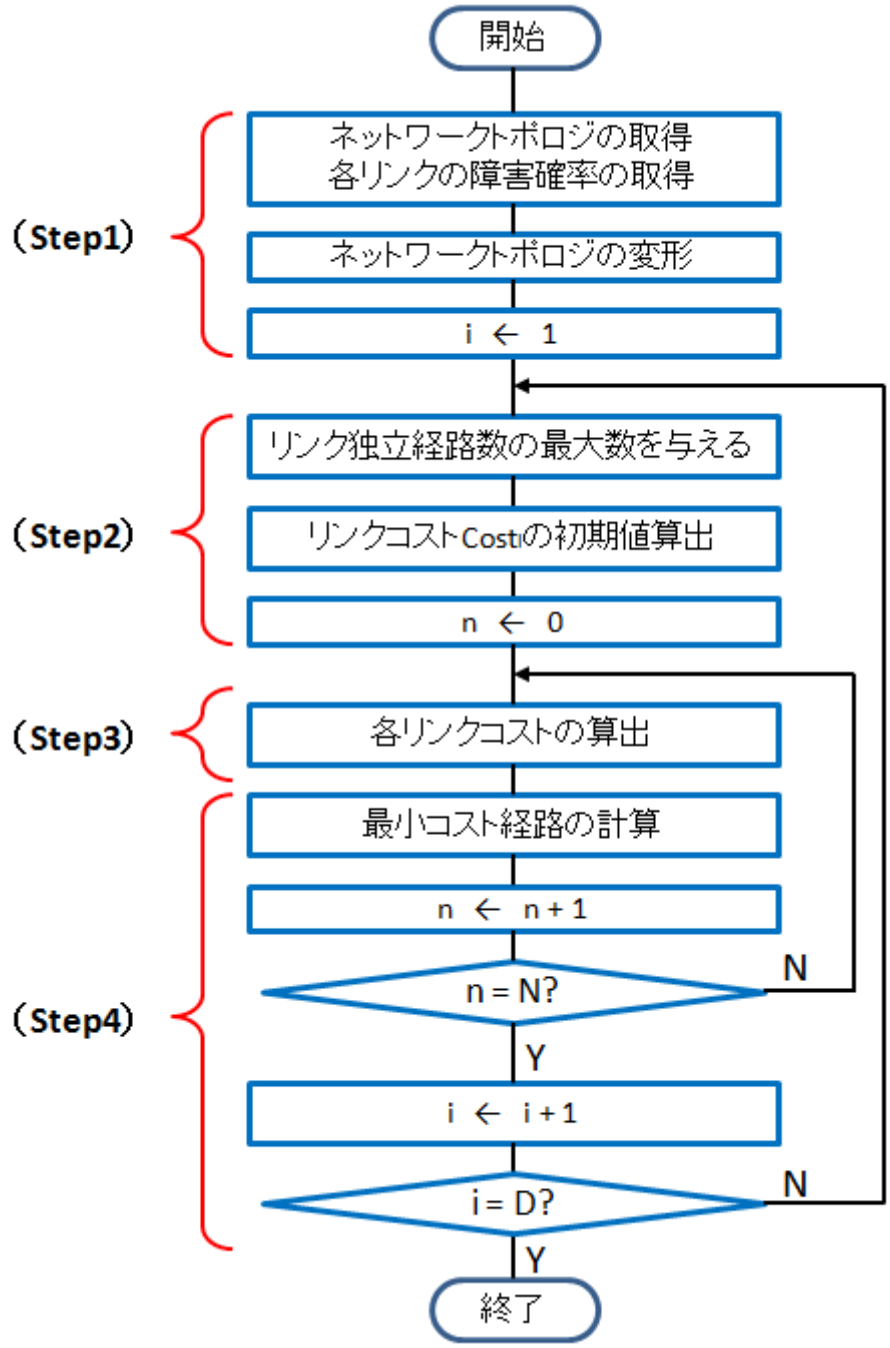

図 3.4：コンテンツ配信経路の計算手順

(Step1)

コンテンツ配信経路計算問題の定式化と同様，図 3.2 に示すネットワークトポロジを図 3.5 の様に変形する．

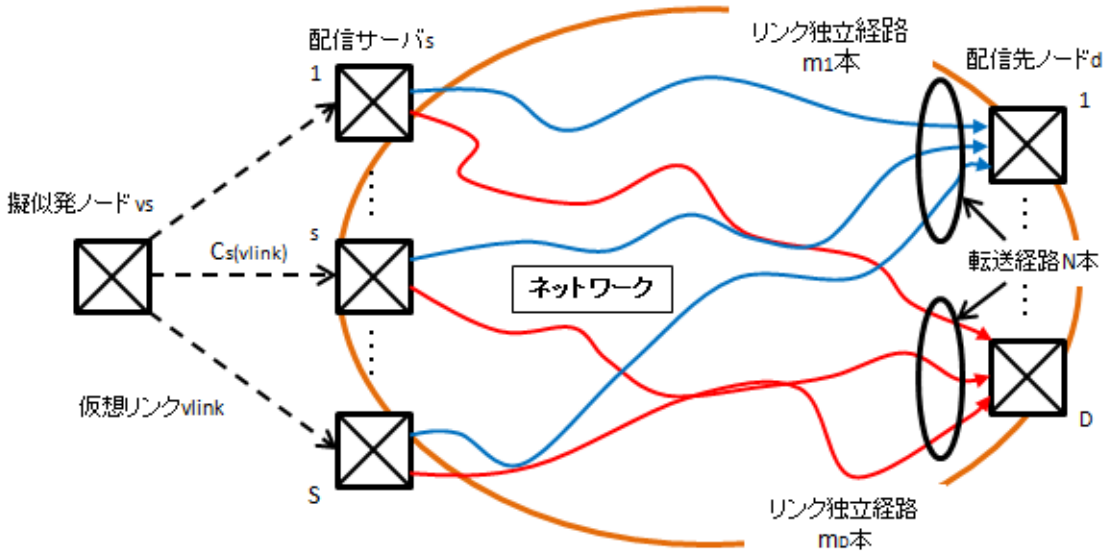

図 3.5：ネットワークトポロジの変形

つまり，新たに擬似発ノード vs を設けて，各配信サーバ s へ仮想リンク接続する．各仮想リンクの障害確率を 0 とし，各仮想リンクの帯域容量は，接続している配信サーバ s が保有しているピース数 $C_{(s)}$に設定する．この様なネットワークトポロジ変形により，各配信サーバが保有するピース数を考慮したコンテンツ配信経路計算が可能となる．

以下の(Step2)から(Step4)を D 個の配信先ノードについて繰り返す．

(Step2)

配信サーバ群から各配信先ノードに至るリンク独立な経路の最大数を m 本とする．このリンク独立な経路本数をもとに，f(=1~m)重リンク障害までを考慮した配信経路算出を行う．また，各リンクコストの初期値は十分小さい値に設定する．

(Step3)

各ピースの配信経路を計算する度にネットワーク全体のリンクコストを更新する．リンクコスト更新手順により，各リンクのコストは，新たに算出対象となる配信経路が当該リンクを通過すると想定した時に，f(=1~m)重リンク障害によって N－K＋1 個以上のピースが損失する確率の増加分に基づき更新される．更新されたリンクコストの下で最小コスト経路を算出することにより，新たな配信経路として，既算出の配信経路とはなるべく重複しない配信経路を計算することが可能となり，N－K＋1 個以上のピースが損失する確率を最小化する配信経路の算出が可能となる．つまり，配信経路を算出する度にリンクコストの調整を行うことで，高信頼な配信経路を計算できる．リンクコストの更新方法に関しては，次節にて具体的に説明する．

(Step4)

(Step3)で更新されたリンクコストの下で，ダイクストラ法を用いて最小コスト経路を算出する．更新されたリンクコストの下で，N 本の最小コスト経路を 1 本ずつ逐次的に算出することで，コンテンツ配信経路を高速に計算する．

以上の(Step2)から(Step4)を繰り返すことでコンテンツ配信経路の算出を行う．また，コンテンツ配信経路計算の流れについて図 3.6 に示す．

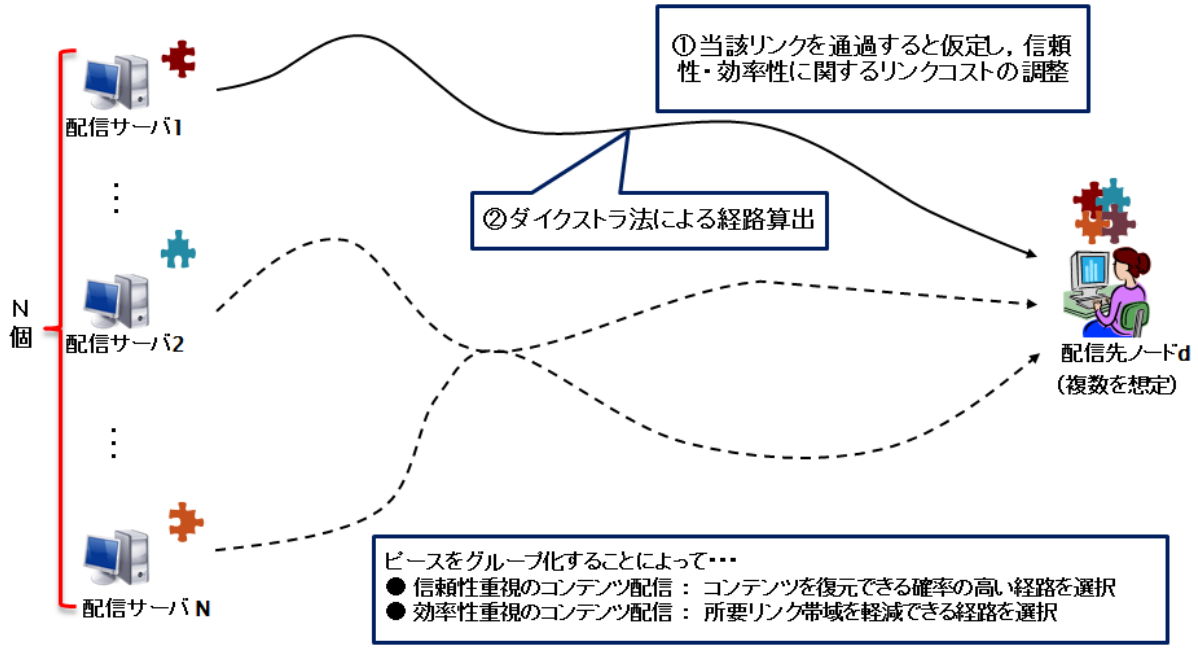

図 3.6：コンテンツ配信経路計算の流れ

3.4　リンクコストの更新法

各ピースの配信経路を算出する際，既算出の配信経路となるべく重複しない配信経路が算出されるように，ネットワーク全体のリンクコストを更新する．リンクコストの更新は，図 3.7 に示すフローチャートに従って行う．まず，全てのリンクに十分小さな値である初期コスト Cost0 を設定する．そして，想定される f 重リンク障害を構成し，かつリンクコストを更新するリンクを含む f 本のリンクの組合せをリストとして構成する．このリストから，1 つずつリンク組合せを取出して，多重リンク障害の発生を想定する．

この時，新たに算出対象となる配信経路が対象リンク l を通過すると想定して，既算出の配信経路本数が N−K 本以下ならば，既算出の配信経路と新たな配信経路に対応するピースの全てが損失となるか否かを判断する．全てのピースが損失する場合，その多重リンク障害確率を対象リンク l のコスト Cost_l に加算する．また，既設の配信経路本数が N−K+1 本以上の場合，既算出の配信経路と新たな配信経路に対応するピースのうち N−K+1 個のピースが損失するか否かを判断する．丁度 N−K+1 個のピースが損失する場合，その多重リンク障害

確率を対象リンク l のコスト $Cost_l$ に加算する．この様な処理を，リスト中の全てのリンク組合せに対して実行する．

全てのリンク組合せを取出した後，最初に設定した初期リンクコスト Cost0 の値が変化していなければ，f の値を 1 加算することで，より多重度の大きいリンク障害を想定してリンクコストの更新を行う．以上述べた処理を，最初は f=1 に設定して行い，f＞m になるまで繰り返し実行する．

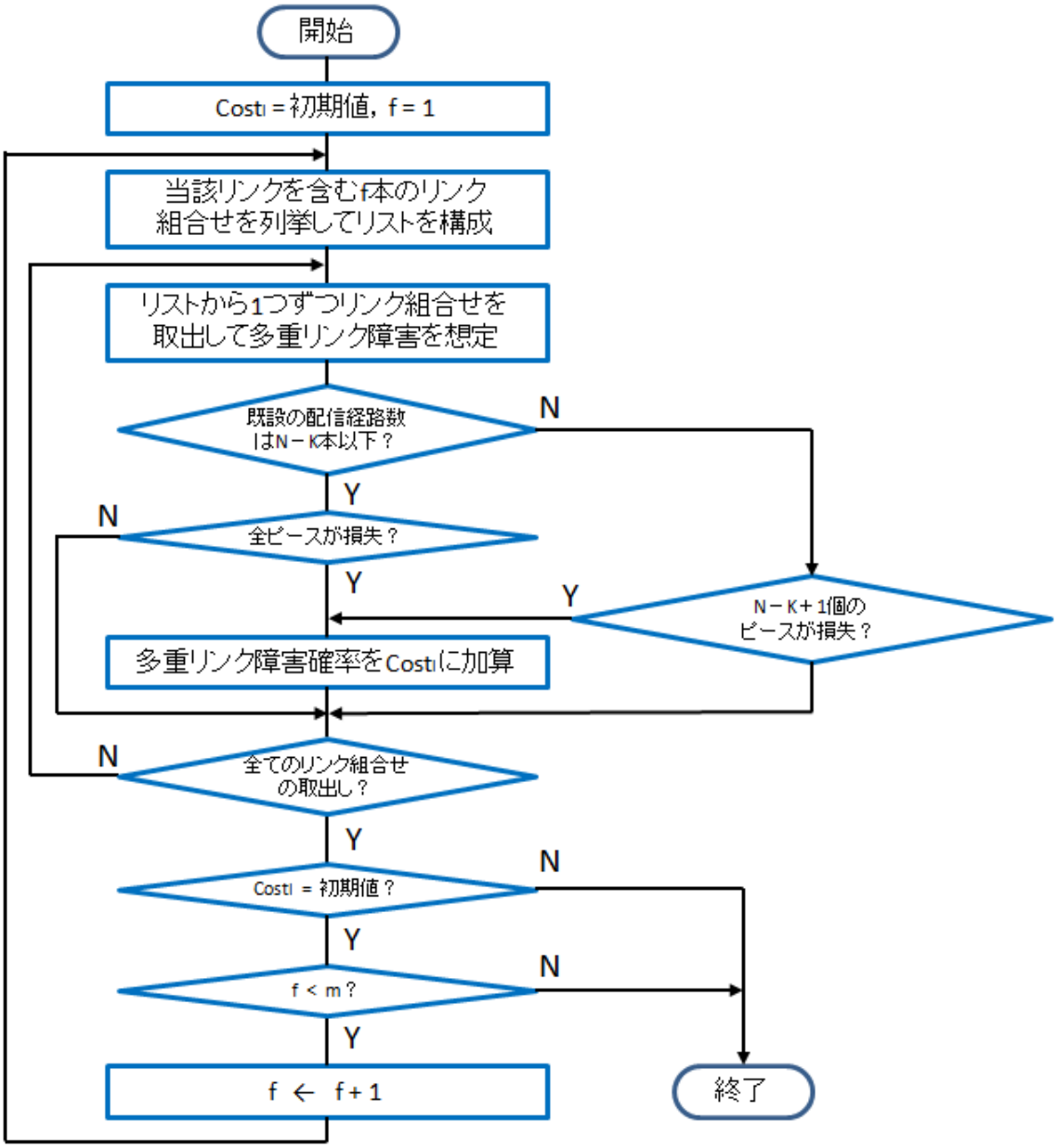

図 3.7：リンクコストの算出手順

リンクコストの更新法に関する具体的な例について，図 3.8 に示す.

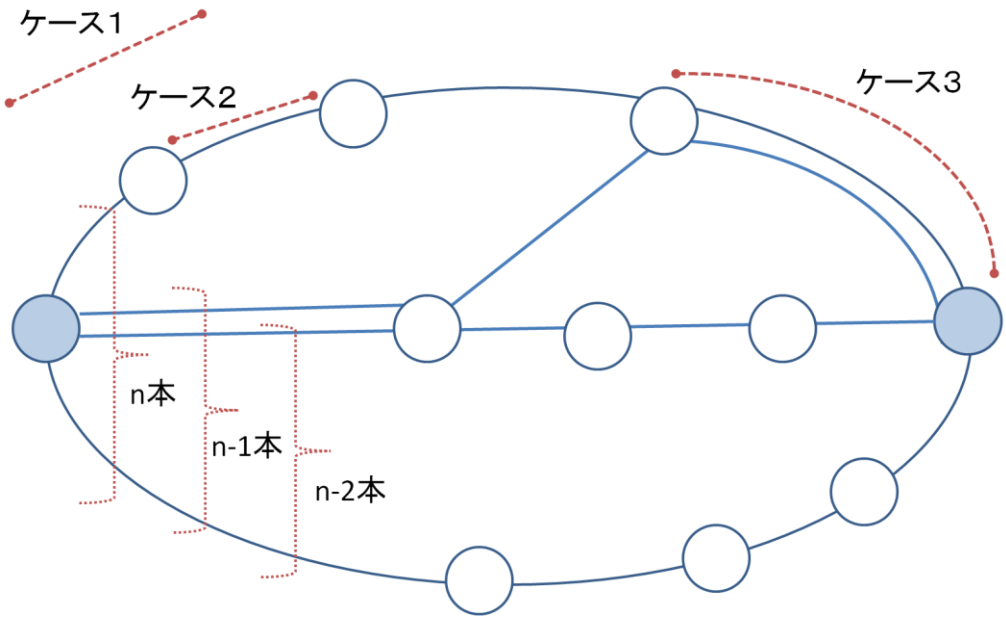

図 3.8：リンクコストの更新例

まず，障害確率を以下の様に表す．

- P(n,f)：n 本の経路の内，f 本以上の経路が障害になる確率
- P(n,f/l)：リンク l が正常，かつ n 本の経路の内，f 本以上の経路が障害になる確率
- P_l：リンク l の障害確率

既に n 本の経路が算出されており，n＋1 本目の経路を算出する際のリンクコスト更新法を説明する．n=1~N－K の時，リンク l のコストは，n＋1 本目の経路がリンク l のみを通過することによって，n＋1 本の経路全てが障害になる確率に設定される．つまり，リンク l のコストは式(13)の様に与えられる．

$$\mathrm{Cost}_l = P(n+1, n+1) \qquad (13)$$

また，ケース 1 の様に n 本の経路の内，リンク l を経路が 1 本も通過していない場合，式(14)が成り立つ．

$$P(n+1, n+1) = P(n, n) \times P_l \qquad (14)$$

続いてケース 2 の様に n 本の経路の内，リンク l を 1 本の経路が通過している場合，式(15)が成り立つ．

$$P(n+1, n+1) = P(n-1, n-1) \times P_l \qquad (15)$$

更にケース 3 の様に n 本の経路の内，リンク l を 2 本の経路が通過している場合，式(16)が成り立つ．

$$P(n+1,n+1) = P(n-2,n-2) \times P_l \qquad (16)$$

同様に，n 本の経路の内，x 本の経路がリンク l を通過している場合，式(17)が成り立つ．

$$P(n+1,n+1) = P(n-x,n-x) \times P_l \qquad (17)$$

従って，リンク l のコストは，リンク l を通過しない n－x 本の経路の全てが障害となる確率とリンク l の障害確率との積として更新される．

n=N－K＋1~N－1 の時，リンク l のコストは，n＋1 本目の経路がリンク l を通過する事によって，N－K＋1 本の経路が障害になる確率の増加分に設定される．つまり，リンク l のコストは式(18)の様に与えられる．

$$Cost_l = P(n+1,f) - P(n,f) \ ,\ f = N - K + 1 \qquad (18)$$

また, ケース 1 のように n 本の経路の内, リンク l を経路が 1 本も通過してない場合, 式(19)が成り立つ．

$$P(n+1,f) = P(n,f/l) + P(n,f-1) \times P_l$$
$$P(n,f) = P(n,f/l) + P(n,f) \times P_l \text{ より，}$$
$$P(n+1,f) = P(n,f) + \{P(n,f-1) - P(n,f)\} \times P_l \qquad (19)$$

続いてケース 2 の様に n 本の経路の内，リンク l を 1 本の経路が通過している場合，式(20)が成り立つ．

$$P(n+1,f) = P(n,f/l) + P(n-1,f-2) \times P_l$$
$$P(n,f) = P(n,f/l) + P(n-1,f-1) \times P_l \text{ より，}$$
$$P(n+1,f) = P(n,f) + \{P(n-1,f-2) - P(n-1,f-1)\} \times P_l \qquad (20)$$

更にケース 3 の様に n 本の経路の内，リンク l を 2 本の経路が通過している場合，式(21)が成り立つ．

$$P(n+1,f) = P(n,f/l) + P(n-2,f-3) \times P_l$$
$$P(n,f) = P(n,f/l) + P(n-2,f-2) \times P_l \text{ より，}$$
$$P(n+1,f) = P(n,f) + \{P(n-2,f-3) - P(n-2,f-2)\} \times P_l \qquad (21)$$

同様に，n 本の経路の内，x 本の経路がリンク l を通過している場合，式(22)が成り立つ．

$$P(n+1,f) = P(n,f) + \{P(n-x,f-x-1) - P(n-x,f-x)\} \times P_l \qquad (22)$$

よって，リンク l のコストは，リンク l を通過しない n－x 本の経路の内，N－K＋1 本の配信経路が障害となる場合に組合せに応じた障害確率の増加分をリンク l に加算することで更新される．

4. 提案コンテンツ配信法の性能評価

本章では，評価対象ネットワークとして用いる NSF(National Science Foundation)ネットワークと実規模ランダムネットワークについて説明する．そして，これら 2 種類のネットワークを用いた提案コンテンツ配信法の性能評価方法及び評価結果について述べる．

4.1 評価対象ネットワーク

本節では，2 種類の評価対象ネットワークである NSF ネットワークと実規模ランダムネットワークに関しての設定条件について説明する．

4.1.1 NSF ネットワーク

評価対象ネットワークとして，図 4.1.1 に示す NSF(National Science Foundation)ネットワークモデルを用いる．NSF ネットワークは，主要なインターネットバックボーンの一部として運用されていた北米のコンピュータネットワークである．このネットワークは，14 ノードからなるネットワークトポロジを有する．図中には，各ノードを識別するために，各ノードに文字を付与している．ここで，全てのリンク障害確率を 0.001 とする．また，各リンクの帯域容量は無限大と仮定して，制約に含めない．更に，NSF ネットワークでは，配信サーバから 1 ホップで配信先ノードに到達する場合を評価対象から除外する．つまり，配信サーバ及び配信先ノードは 2 ホップ以上の間隔を置いて選択する．

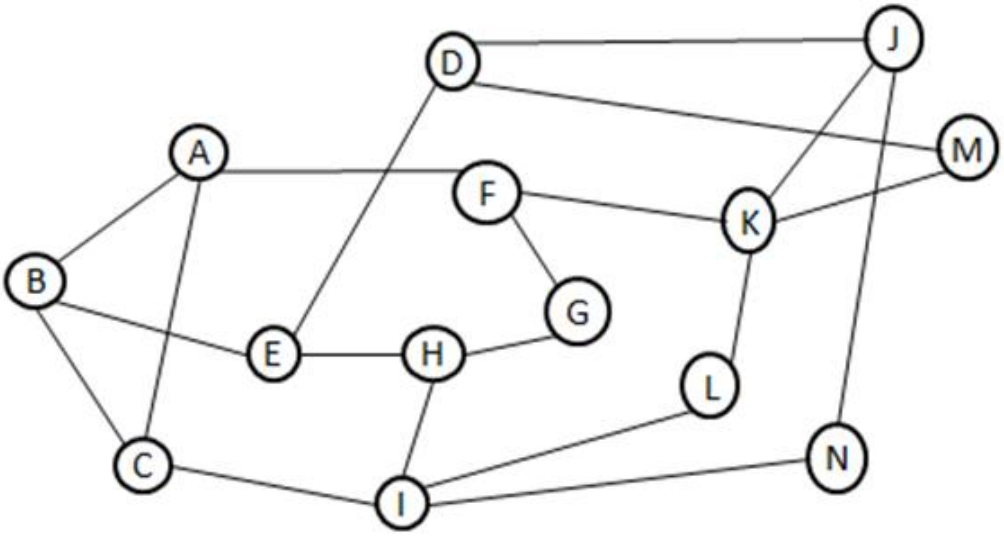

図 4.1.1：NSF ネットワークモデル

4.1.2　実規模ランダムネットワーク

提案するコンテンツ配信法の有効性を評価するために，実規模ランダムネットワークを評価対象ネットワークとする．今回，ノード数が 100 のランダムネットワークを生成して評価する．また，ランダムネットワークにおいて，平均ノード次数は 4.0 に固定し，全てのリンク障害確率は 0.001 であると仮定する．また，各リンクの帯域容量は無限大と仮定して，制約に含めない．更に，配信サーバと配信先ノード間のリンク独立な経路本数が 3 本となるように配信サーバと配信先ノードを選択し，配信サーバと配信先ノードの間隔が最低でも 2 ホップ以上になるようにする．全てのリンクのコスト初期値は十分小さい値を設定する．表 4.1.2 に，生成したランダムネットワークの設定条件について示す．

表 4.1.2：生成したランダムネットワークの設定条件

ノード数	100
リンク数	400
平均ノード次数	4.0
リンク障害確率	0.001
リンクの初期コスト	十分小さい値

4.2　評価方法

評価を行う上で，リンク帯域容量の計算方法やリンク障害によるピースの損失率の求め方について説明する．また，評価中に変化させる条件である配信経路の計算順序やピースのグルーピング方法について説明する．そして，各評価対象ネットワークにおける具体的な評価方法について示す．尚，いずれも評価環境として，Intel(R)Core(TM)2 Duo CPU E8500 @ 3.16GHz，メモリ 4.00GB のコンピュータを使用する．

4.2.1　リンク帯域容量の計算方法

グループ別にネットワーク符号化を適用すれば，各中継ノードで同一グループに属し，配信先ノードが異なる複数のピースを 1 つのピースにまとめて出リンクから転送することができる．つまり，同一グループに属している異なる配信先ノードに転送される複数のピースは，互いに出リンク帯域を共用することができる．従って，各リンクの帯域容量は，各グループにおいて当該リンクを通過して各配信先ノードに至る配信経路数の最大数を算出し，算出した最大数を全グループについて加算した値となる．リンク帯域容量として，閾値秘密分散保持されたコンテンツを構成する各ピースを複数の配信先ノードへ配信するために必要なリンク帯域の総和を算出する．尚，リンク帯域容量の計算では，1 つのピースの所要リンク帯域を 1.0 として考える．

4.2.2　損失率の計算方法

損失率として，各配信先ノードにおいて元のコンテンツを復元できない確率の平均値を算出する．損失率の計算においては，全てのリンクの障害確率が等しいものと仮定し，更に多重リンク障害の発生確率は，当該多重リンク障害を構成する各リンクの障害確率の積で表されると仮定する．従って損失率は，全てのリンク障害に対する元のコンテンツが復元できない配信先ノード数の総和を求め，配信先ノード数で除算したものに，リンク障害確率を掛けた値となる．本研究での評価では，1 重リンク障害または 2 重リンク障害を想定した場合についての損失率を求める．もし，1 重リンク障害を想定した場合の損失率が 0 の場合は，2 重リンク障害についての計算を行う．なお，3 重リンク障害が発生する確率は非常に小さいと考えられるため，今回の評価では考慮しないものとする．

4.2.3　配信経路の計算順序

複数の配信サーバに閾値秘密分散保持されているコンテンツを構成する各ピースに対する配信経路について，2 種類の計算順序を考慮する．計算順序 1 は，同一配信サーバ内に保持されている全てのピースの配信経路を優先的に計算する方法である．計算順序 2 は，異なる配信サーバ内に保持されているピースの配信経路を優先的に計算する方法である．以上の 2 種類の計算順序を変化させて評価を行う．表 4.2.3 に計算順序 1 と計算順序 2 に関して説明し，その概要を図 4.2.4 に示す．

表 4.2.3：計算順序の概要

計算順序 1	同一サーバ内のピースの配信経路を優先的に算出
計算順序 2	異なるサーバ内のピースの配信経路を優先的に算出

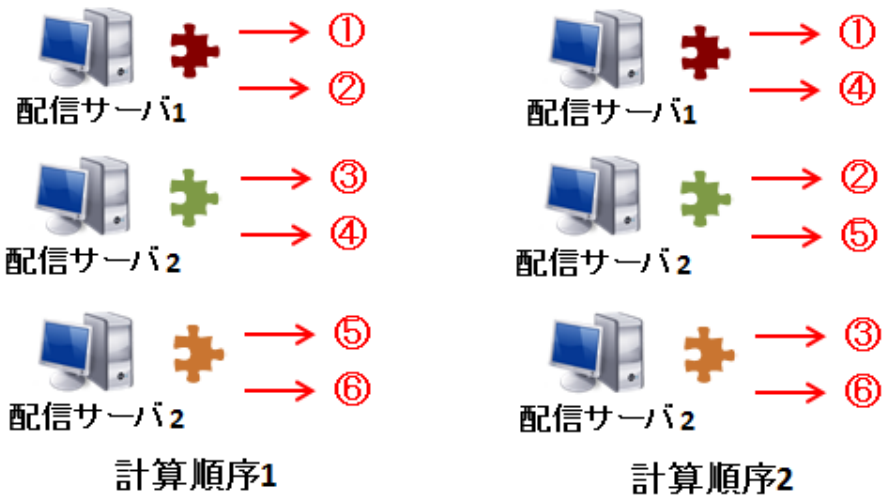

図 4.2.4：配信経路の計算順序

4.2.4　ピース群のグルーピング方法

ピースのグループ分割の方法として，表 4.2.5 に示す 2 種類の方法に基づいたグループ分けを行う．グループ化 1 は，同一配信サーバに保持されているピースをグループ化する方法である．グループ化 2 は，異なる配信サーバに保持されているピースをグループ化する方法である．以上の 2 種類のグルーピング法を変化させて評価を行う．表 4.2.5 にピースのグルーピング法に関して説明し，図 4.2.6 にグルーピング法の概要を示す．

表 4.2.5：グルーピ化の概要

グループ化 1	同一サーバ内のピースをまとめてグループ化
グループ化 2	異なるサーバ内のピースをグループ化

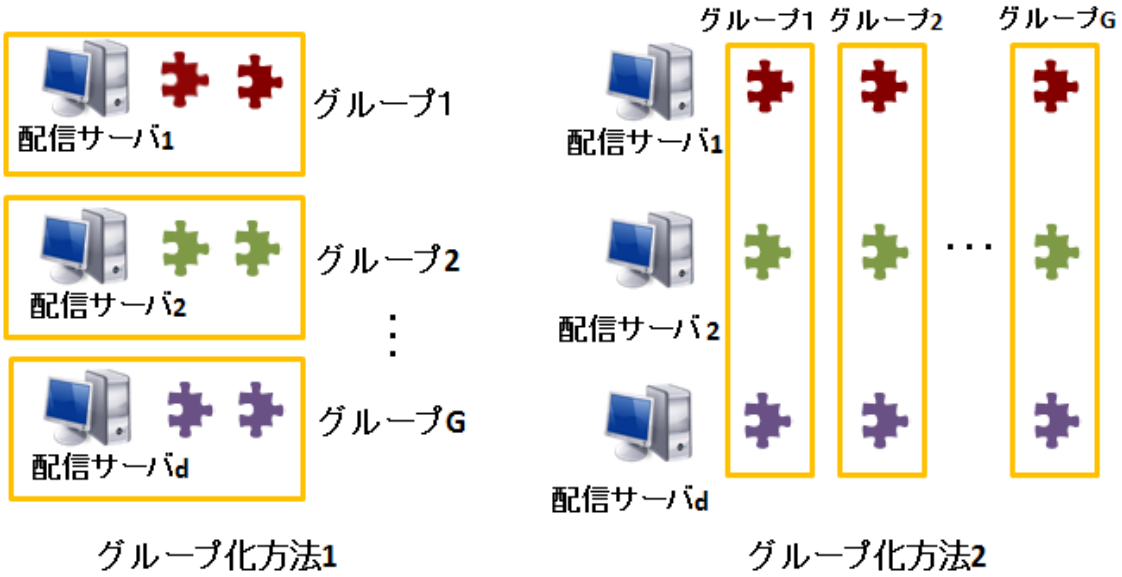

図 4.2.6：ピースのグルーピング方法

4.2.5　NSF ネットワークでの評価方法

図 4.1.1 に示す NSF ネットワークにおいて，配信サーバ 3 つと配信先ノード 3 つの位置を変化させた 5 ケースについて評価する．ここで，元のコンテンツを構成するピース群は 9 ピース(N=9)であり，各配信サーバは，それぞれピースを 3 ピースずつ保持する．また，閾値秘密分散法における閾値の値は 6(K=6)であり，6 ピース以上のピースを集めると元のコンテンツを復元することが可能である．

評価を行う際，ピース群を分けるグループ数を変化させながら，信頼性を重視する配信経路計算と効率性を重視する配信経路計算に関するリンク帯域容量と損失率を求める．ここで，信頼性を重視する配信経路計算法は，3.2 節で提案したコンテンツ配信経路計算法を指す．一方，効率性を重視する配信経路計算法は，所要リンク帯域の最小化を目的とした方法であり，

逐次的に最小コスト経路計算を行う際に，新たに配信経路を計算するピースと同一グループに所属するピースを異なる配信先ノードに転送するための配信経路が既に通過しているリンクのコストは十分小さな値に設定し，他のリンクのコストは 1.0 に設定する．リンク帯域容量と損失率に関しては，前節で述べた計算方法によって求める．表 4.2.7 に，NSF ネットワークにおける評価条件を示す．また，配信サーバと配信先ノードの位置関係について，異なる 5 ケースを以下に示す．

- 配信サーバが A，B，C で，配信先ノードが J，M，Nの場合
- 配信サーバが A，C，H で，配信先ノードが J，M，N の場合
- 配信サーバが I，K，N で，配信先ノードが A，B，D の場合
- 配信サーバが A，B，N で，配信先ノードが D，G，H の場合
- 配信サーバが E，I，M で，配信先ノードが A，F，J の場合

表 4.2.7：NSF ネットワークの評価条件

配信サーバ数	3
配信先ノード数	1，3
合計ピース数	N = 9
各配信サーバのピース保持数	3 ピース
復元に必要なピース数	K = 6
グループ数	G = 1，3，9
配信経路の計算順序	計算順序 1，計算順序 2
ピースのグルーピング法	グループ化 1，グループ化 2

4.2.6　実規模ランダムネットワークでの評価方法

ノード数が 100 であるランダムネットワークにおいて，配信サーバ 3 つと配信先ノード 3 つの場合と，配信サーバ 4 つと配信先ノード 4 つの場合とについて，配信サーバと配信先ノードの位置を変化させた 5 ケースについて評価する．元のコンテンツを構成するピース群は 9 ピース(N=9)または 16 ピース(N=16)であり，各配信サーバは，それぞれ 3 ピースまたは 4 ピースずつ保持する．また，閾値秘密分散法における閾値の値は，6(K=6)または 8(K=8)または 12(K=12)とし，6 ピース以上または 8 ピース以上または 12 ピース以上のピースを集めると元のコンテンツを復元することが可能となる．

評価を行う際，ピース群を分けるグループ数を変化させながら，信頼性を重視する配信経路計算と効率性を重視する配信経路計算に関するリンク帯域容量と損失率を求める．リンク帯域容量と損失率に関しては，前節に述べた計算方法によって求める．表 4.2.8 に，実規模ランダムネットワークにおける評価条件を示す．

表 4.2.8：実規模なランダムネットワークの評価条件

配信サーバ数	3，4
配信先ノード数	1，2，3，4
合計ピース数	N = 9，16
各配信サーバのピース保持数	3 ピース，4 ピース
復元に必要なピース数	K = 6，8，12
グループ数	G = 1，2，3，4，8，9，16
配信経路の計算順序	計算順序 1，計算順序 2
ピースのグルーピング法	グループ化 1，グループ化 2

4.3　評価結果

本節では，NSF ネットワークと実規模ランダムネットワークを用いた提案コンテンツ配信法の性能評価結果を示す．

4.3.1　NSF ネットワークでの評価結果

NSF ネットワークにおいて，配信サーバと配信先ノードの位置が異なる 5 つのケースについて評価した結果を表 4.3.1(a)~ (e)に示す．複数の配信先は，コンテンツを 3 つの配信先ノードに同時配信した場合の結果を示し，個別の配信先は，個別の配信先ノードに対してのみコンテンツを配信した結果をまとめたものである．また，各ケースの損失率を計算する際，1 重リンク障害において損失率 0 である場合は，2 重リンク障害についての損失率を求めた．リンク帯域と損失率に関しては，4.2.1 節と 4.2.2 節で定義した計算方法によって算出された値である．

表 4.3.1(a)：配信サーバ A，B，C で配信先ノード J，M，N の評価結果

配信先ノード	設定条件	信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	54	7.33	39	9
	G=1，計算順序2	54	7.33	39	9
	G=3，計算順序1，グループ化1	63	1 重:0 2 重:36	42	0.33
	G=3，計算順序1，グループ化2	72	3.33	39	9
	G=3，計算順序2，グループ化1	63	1 重:0 2 重:36	42	0.33
	G=3，計算順序2，グループ化2	74	7	39	9
	G=9，計算順序1	72	1 重:0 2 重:86	42	0.33
	G=9，計算順序2	64	1 重:0 2 重:91.7	42	0.33
個別の配信先	G=9，計算順序1	110	1 重:0 2 重:86	78	1 重:0.67 2 重:27
	G=9，計算順序2	115	1 重:0 2 重:91.7	78	1 重:0.67 2 重:27

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.1(b)：配信サーバ A，C，H で配信先ノード J，M，N の評価結果

配信先ノード	設定条件	信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	51	7.33	39	9
	G=1，計算順序2	49	8	39	9
	G=3，計算順序1，グループ化1	72	1 重:0 2 重:36.3	42	0.33
	G=3，計算順序1，グループ化2	67	4.33	39	9
	G=3，計算順序2，グループ化1	72	1 重:0 2 重:36.3	42	0.33
	G=3，計算順序2，グループ化2	56	3.33	39	9
	G=9，計算順序1	73	1 重:0 2 重:87	42	0.33
	G=9，計算順序2	74	1 重:0 2 重:72	42	0.33
個別の配信先	G=9，計算順序1	115	1 重:0 2 重:87	75	1 重:0.67 2 重:27
	G=9，計算順序2	106	1 重:0 2 重:72	75	1 重:0.67 2 重:27

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.1(c)：配信サーバ I，K，N で配信先ノード A，B，D の評価結果

配信先ノード	設定条件	信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	51	5.67	48	6
	G=1，計算順序2	51	5.67	48	6
	G=3，計算順序1，グループ化1	54	1 重:0 2 重:22	48	1.67
	G=3，計算順序1，グループ化2	64	4.33	48	6
	G=3，計算順序2，グループ化1	54	1 重:0 2 重:22	48	1.67
	G=3，計算順序2，グループ化2	59	3.67	48	6
	G=9，計算順序1	77	1 重:0 2 重:60	48	1.67
	G=9，計算順序2	71	1 重:0 2 重:61	48	1.67
個別の配信先	G=9，計算順序1	96	1 重:0 2 重:60	66	1.67
	G=9，計算順序2	96	1 重:0 2 重:61	66	1.67

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.1(d)：配信サーバ A，B，N で配信先ノード D，G，H の評価結果

配信先ノード	設定条件	信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	48	5.33	45	5.67
	G=1，計算順序2	48	5.33	45	5.67
	G=3，計算順序1，グループ化1	72	0.33	45	1.67
	G=3，計算順序1，グループ化2	67	3.67	45	5.67
	G=3，計算順序2，グループ化1	72	0.33	45	1.67
	G=3，計算順序2，グループ化2	62	4.67	45	5.67
	G=9，計算順序1	74	0.67	45	1.67
	G=9，計算順序2	74	0.67	45	1.67
個別の配信先	G=9，計算順序1	112	0.67	66	1.67
	G=9，計算順序2	93	0.67	66	1.67

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.1(e)：配信サーバ E，I，M で配信先ノード A，F，J の評価結果

配信先ノード	設定条件	信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	42	6.33	39	6.67
	G=1，計算順序2	42	6.33	39	6.67
	G=3，計算順序1，グループ化1	48	1重:0 2重:16.3	42	0.33
	G=3，計算順序1，グループ化2	66	1.67	39	6.67
	G=3，計算順序2，グループ化1	48	1重:0 2重:16.3	42	0.33
	G=3，計算順序2，グループ化2	56	3.67	39	6.67
	G=9，計算順序1	69	1重:0 2重:52.7	42	0.33
	G=9，計算順序2	67	1重:0 2重:44.7	42	0.33
個別の配信先	G=9，計算順序1	91	1重:0 2重:52.7	63	0.33
	G=9，計算順序2	83	1重:0 2重:44.7	63	0.33

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.1(a)~(e)の結果から，閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに個別に配信する場合と比較して，複数の配信先ノードに同時配信することにより，所要リンク帯域容量が減少し，効率的なコンテンツ配信を実現できる．また，提案コンテンツ配信法では，グループ数の増加に伴い，信頼性が向上するが効率性が低下する．更に，信頼性を重視した配信経路計算と効率性を重視した配信経路計算を比較すると，信頼性を重視した配信経路計算では，所要リンク帯域容量が増加するが，ピースの損失率が低くなることが分かる．一方，効率性を重視した配信経路計算では，所要リンク帯域容量は小さくなるが，ピースの損失率が大きくなることが分かる．

更にグループ分割数の変化により，所要リンク帯域容量やピースの損失率が大きく変化することも分かる．例えば，信頼性重視の配信経路計算において，グループ数が G=3 や G=9 の時は，単一リンク障害によって元のコンテンツが復元できなくなる状況を回避できる可能性が高くなることが分かる．また，効率性を重視した配信経路計算において，グループ数を G=3 に分割した時，異なる配信サーバに保持されているピースを優先的にグループ化することにより，ネットワーク符号化が促進されて，所要リンク帯域容量が小さくなることが分かる．

従って，提案コンテンツ配信法において，グループ数や配信経路の計算順序，ピース群のグループ化の条件を変えることで，高信頼かつ高効率なコンテンツ配信を実現できる．尚，コンテンツ配信経路の計算は，ダイクストラ法の適用によって高速に行うことができた．

NSF ネットワークにおける配信経路の一部について図 4.3.2～4.3.7 に示す．設定条件は，配信サーバが A，B，N で配信先ノードが D，G，H である．また，各配信サーバはピースを 3 ピースずつ保持しており，合計ピース数は 9 ピース(N=9)とする．また，元のコンテンツの復元に必要なピース数を 6 ピース(K=6)とし，グループ数 G=3 について計算順序 1 とグループ化 1 及びグループ数 G=3 について計算順序 1 とグループ化 2 についての配信経路を示す．ここで図中の同一色の経路は同じグループに属するピースを示す．

図 4.3.2(a)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における信頼性重視のコンテンツ配信経路の中の配信先ノード D への経路を示したものである． 各ピースの配信経路は，グループごとに重複しない経路を通っていることが分かる．

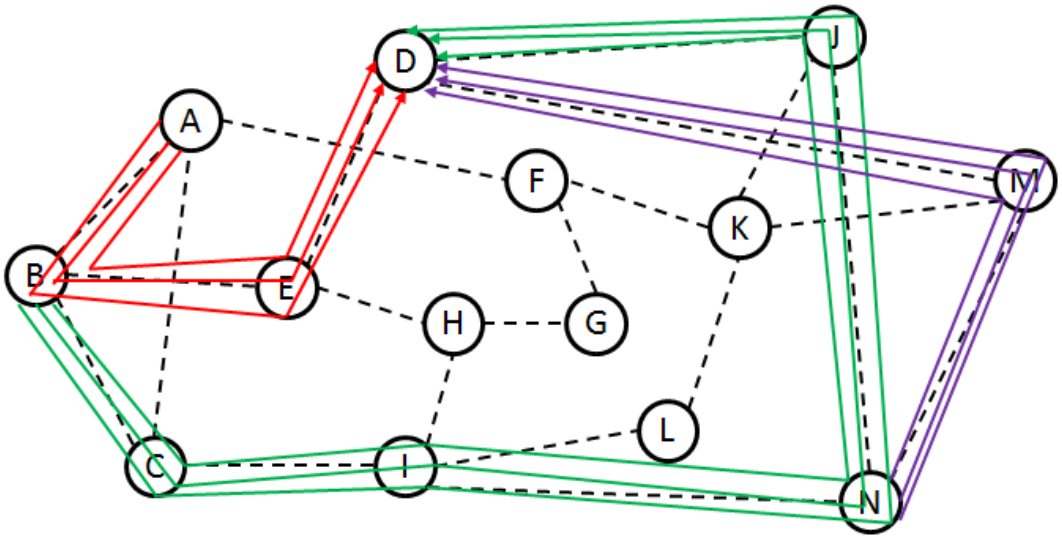

図 4.3.2(a)：配信先ノード D に関する信頼性重視のコンテンツ配信経路

図 4.3.2(b)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における信頼性重視のコンテンツ配信経路の中の配信先ノード G への経路を示したものである．各ピースの配信経路は，グループごとに極力重複しない経路を通っていることが分かる．

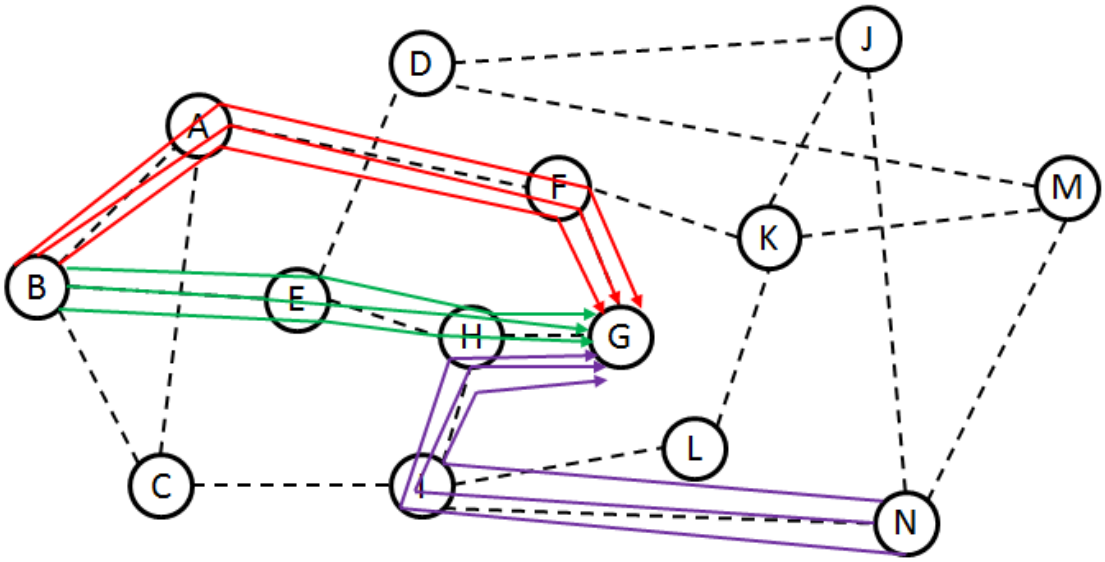

図 4.3.2(b)：配信先ノード G に関する信頼性重視のコンテンツ配信経路

図 4.3.2(c)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における信頼性重視のコンテンツ配信経路の中の配信先ノード H への経路を示したものである．各ピースの配信経路は，グループごとに重複しない経路を通っていることが分かる．

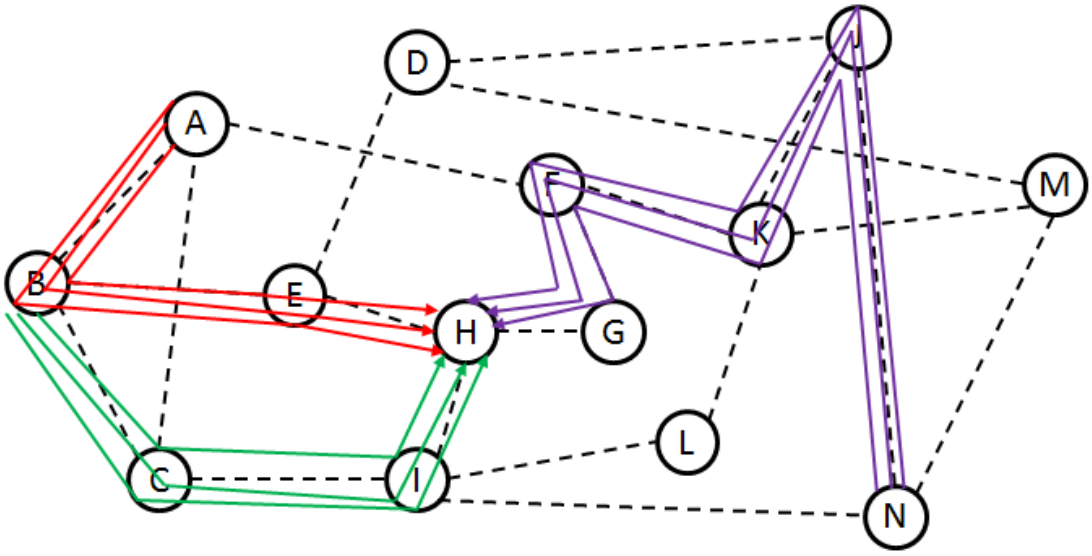

図 4.3.2(c)：配信先ノード H に関する信頼性重視のコンテンツ配信経路

図 4.3.3(a)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における信頼性重視のコンテンツ配信経路の中のグループ 1 のみの経路を示したものである．この配信経路から配信サーバ A から配信されるピースが中継ノード B でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．

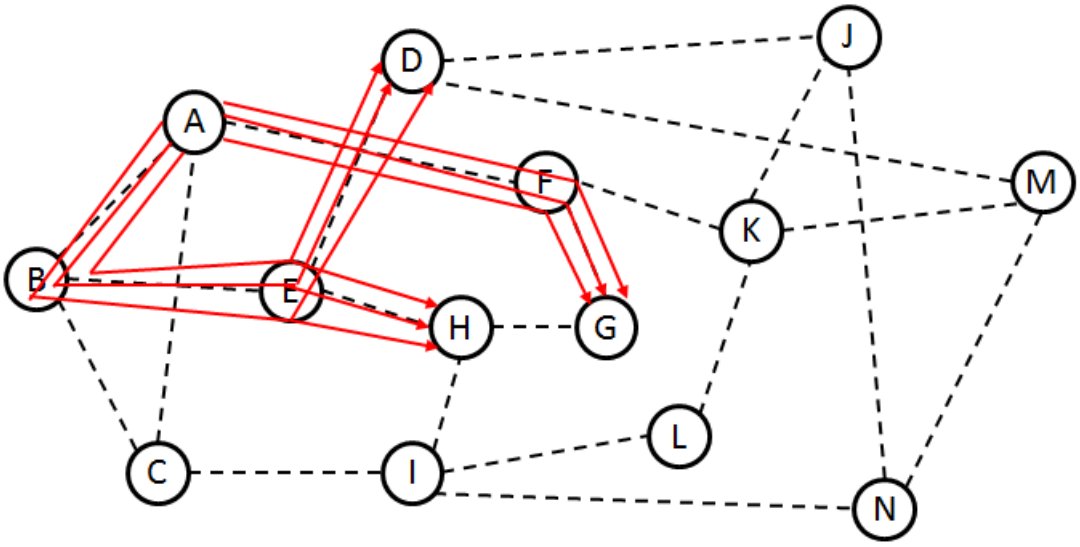

図 4.3.3(a)：グループ 1 に関する信頼性重視のコンテンツ配信経路

図 4.3.3(b)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における信頼性重視のコンテンツ配信経路の中のグループ 2 のみの経路を示したものである．この配信経路から配信サーバ B から配信されるピースが中継ノード C でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．

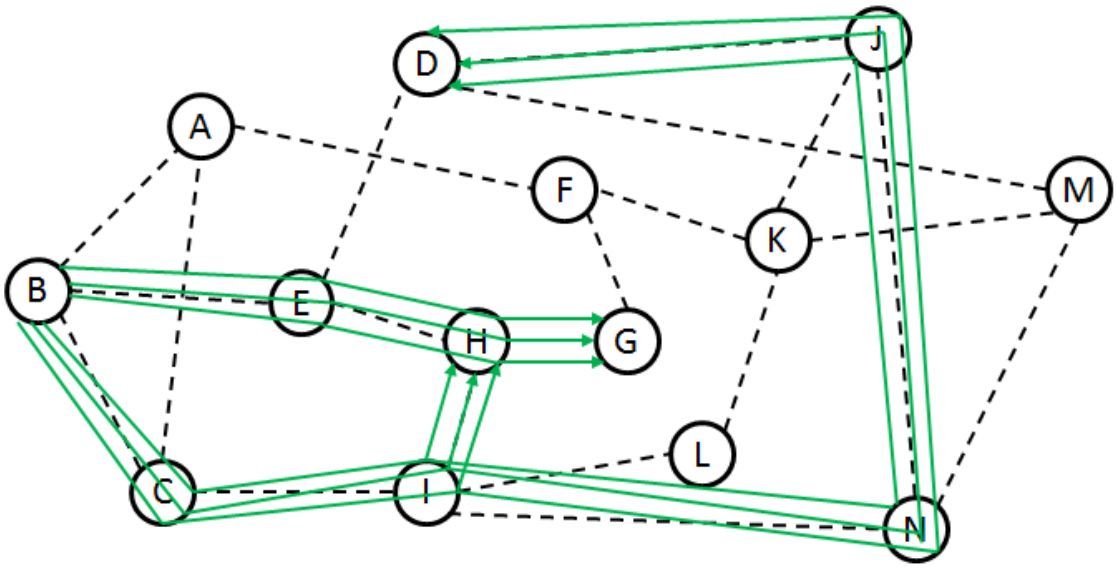

図 4.3.3(b)：グループ 2 に関する信頼性重視のコンテンツ配信経路

図 4.3.3(c)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における信頼性重視のコンテンツ配信経路の中のグループ 3 のみの経路を示したものである．この配信経路から配信サーバ N から配信されるピースはマルチキャスト転送やネットワーク符号化の効果を得ず，配信先ノード D，G，H に配信されていることが分かる．

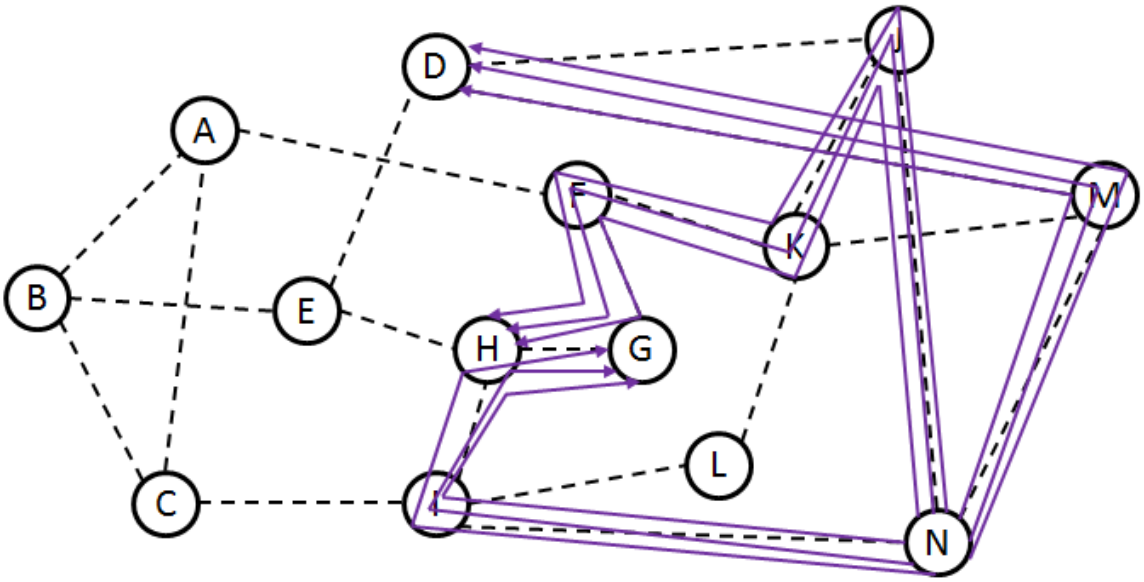

図 4.3.3(c)：グループ 3 に関する信頼性重視のコンテンツ配信経路

図 4.3.4(a)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における効率性重視のコンテンツ配信経路の中のグループ 1 のみの経路を示したものである．この配信経路から配信サーバ A から配信されるピースが中継ノード B でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．

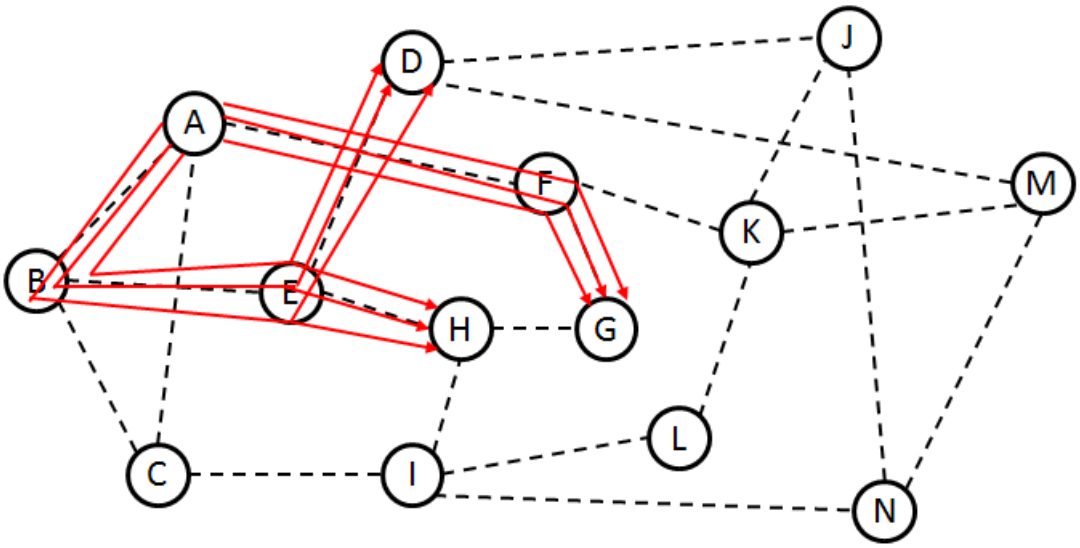

図 4.3.4(a)：グループ 1 に関する効率性重視のコンテンツ配信経路

図 4.3.4(b)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における効率性重視のコンテンツ配信経路の中のグループ 2 のみの経路を示したものである．この配信経路から配信サーバ B から配信されるピースが中継ノード E と中継ノード H でマルチキャスト転送され，異なる配信先ノード D，G，H に配信されていることが分かる．

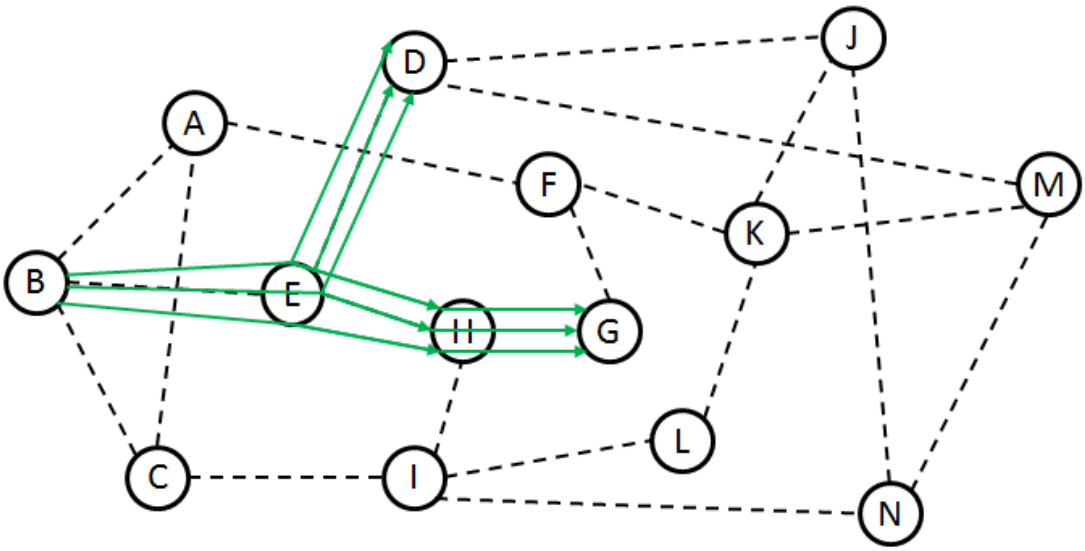

図 4.3.4(b)：グループ 2 に関する効率性重視のコンテンツ配信経路

図 4.3.4(c)は，グループ数 G=3 についての計算順序 1 とグループ化 1 における効率性重視のコンテンツ配信経路の中のグループ 3 のみの経路を示したものである．この配信経路から配信サーバ N から配信されるピースが中継ノード H でマルチキャスト転送され，異なる配信先ノード H，G に配信されていることが分かる．

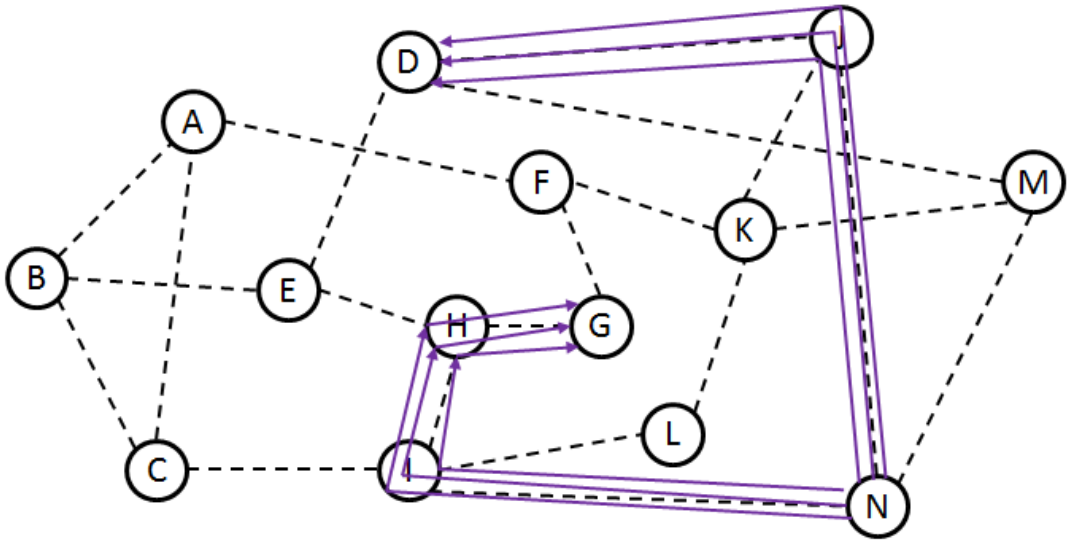

図 4.3.4(c)：グループ 3 に関する効率性重視のコンテンツ配信経路

図 4.3.5(a)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における信頼性重視のコンテンツ配信経路の中の配信先ノード D への経路を示したものである．各ピースの配信経路は，グループごとに極力重複しない経路を通っていることが分かる．

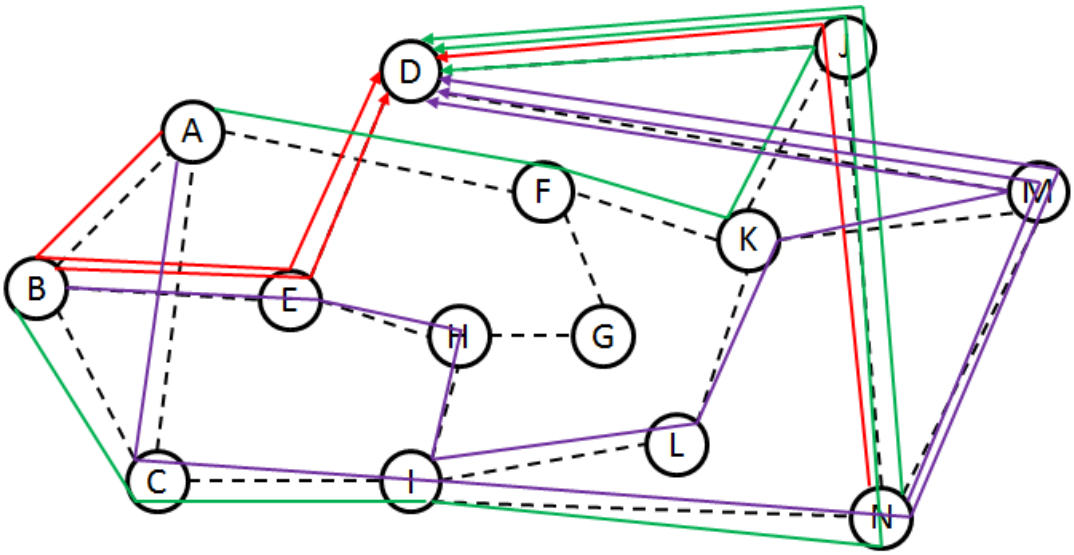

図 4.3.5(a)：配信先ノード D に関する信頼性重視のコンテンツ配信経路

図 4.3.5(b)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における信頼性重視のコンテンツ配信経路の中の配信先ノード G への経路を示したものである．各ピースの配信経路は，グループごとに極力重複しない経路を通っていることが分かる．

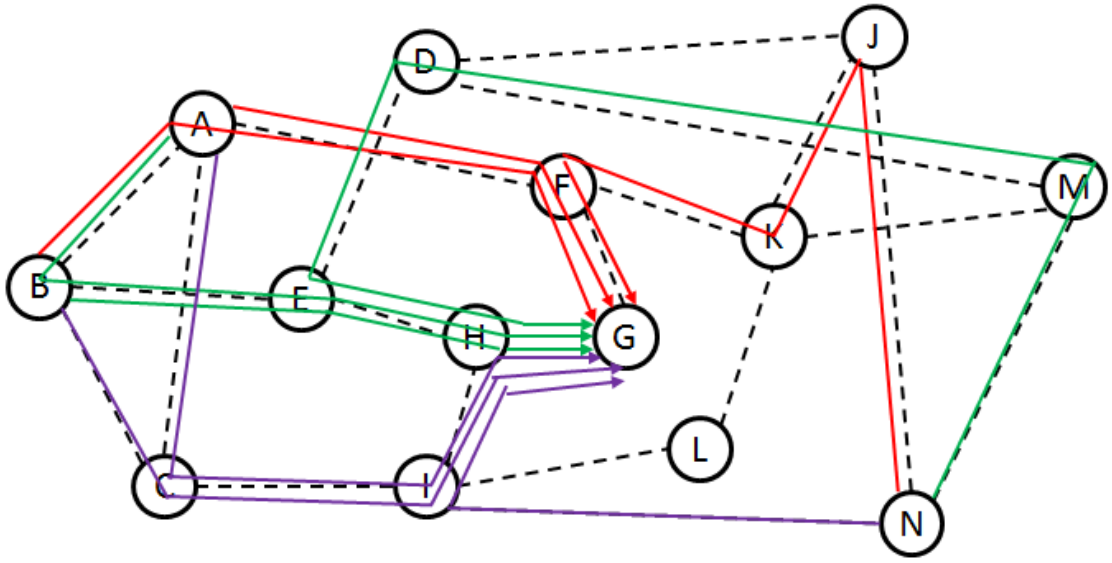

図 4.3.5(b)：配信先ノード G に関する信頼性重視のコンテンツ配信経路

図 4.3.5(c)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における信頼性重視のコンテンツ配信経路の中の配信先ノード H への経路を示したものである．各ピースの配信経路は，グループごとに極力重複しない経路を通っていることが分かる．

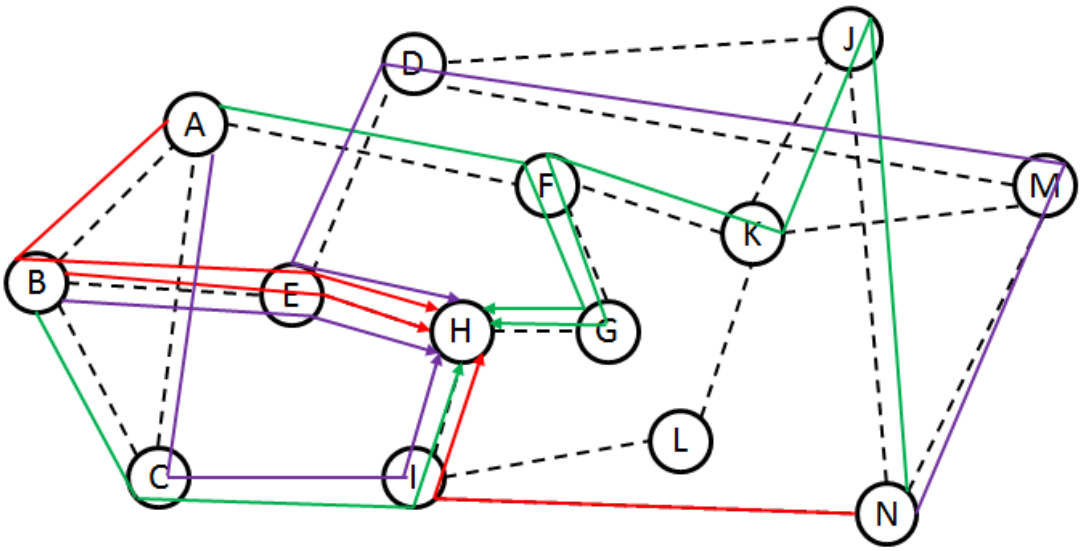

図 4.3.5(c)：配信先ノード H に関する信頼性重視のコンテンツ配信経路

図 4.3.6(a)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における信頼性重視のコンテンツ配信経路の中のグループ 1 のみの経路を示したものである．この配信経路から配信サーバ A から配信されるピースが中継ノード E でマルチキャスト転送され，異なる配信先ノード D，H に配信されることが分かる．更に，配信サーバ B から配信されるピースも中継ノード E でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．また，配信サーバ N から配信されるピースが中継ノード J でマルチキャスト転送され，異なる配信先ノード D，G に配信されていることが分かる．

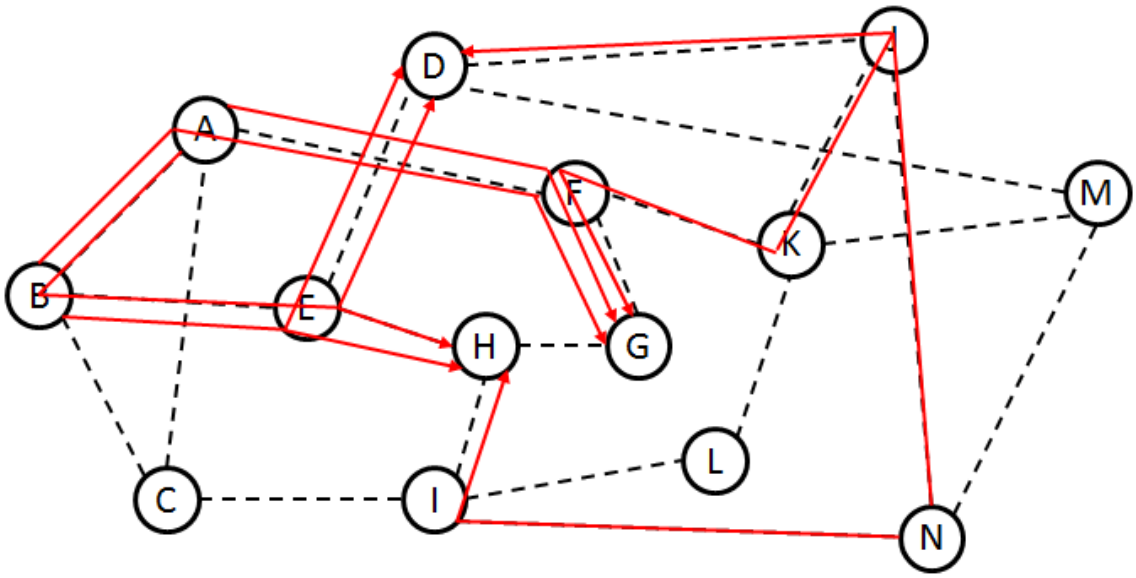

図 4.3.6(a)：グループ 1 に関する信頼性重視のコンテンツ配信経路

図 4.3.6(b)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における信頼性重視のコンテンツ配信経路の中のグループ 2 のみの経路を示したものである．この配信経路から

配信サーバ B から配信されるピースが中継ノード I でマルチキャスト転送されて配信先ノード D，H に配信されていることが分かる．また，配信サーバ A から配信されるピースが中継ノード F でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる. 更に, 配信サーバ N から配信されるピースが中継ノード J でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる.

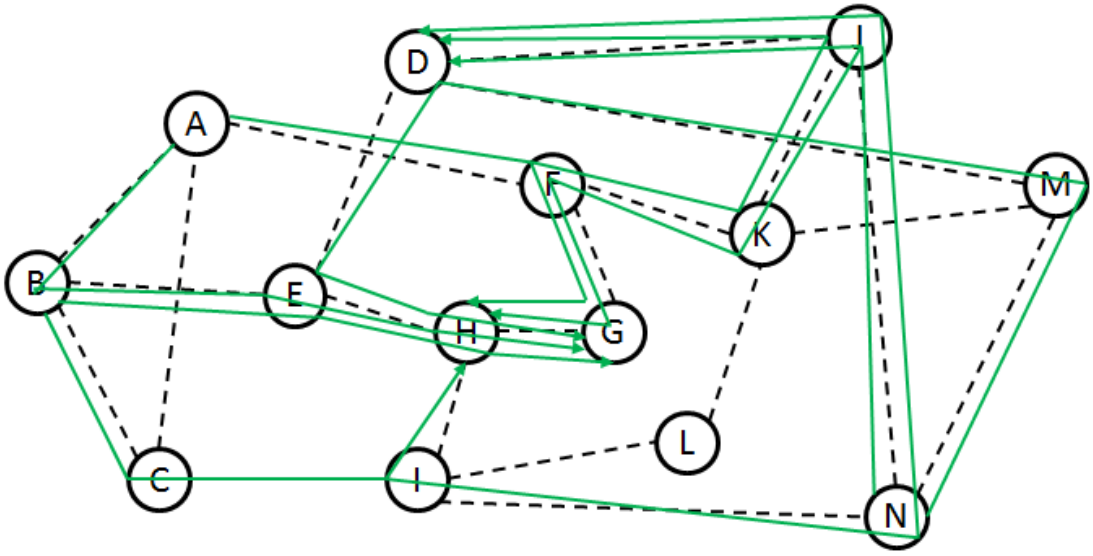

図 4.3.6(b)：グループ 2 に関する信頼性重視のコンテンツ配信経路

図 4.3.6(c)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における信頼性重視のコンテンツ配信経路の中のグループ 3 のみの経路を示したものである．この配信経路から配信サーバ A から配信されるピースが中継ノード I と中継ノード H でマルチキャスト転送され，配信先ノード D，G，H に配信されていることが分かる．また配信サーバ B から配信されるピースが中継ノード H でマルチキャスト転送され，配信先ノード D，H に配信されていることが分かる．更に配信サーバ N から配信されるピースが中継ノード D でマルチキャスト転送され，配信先ノード D，H に配信されていることが分かる.

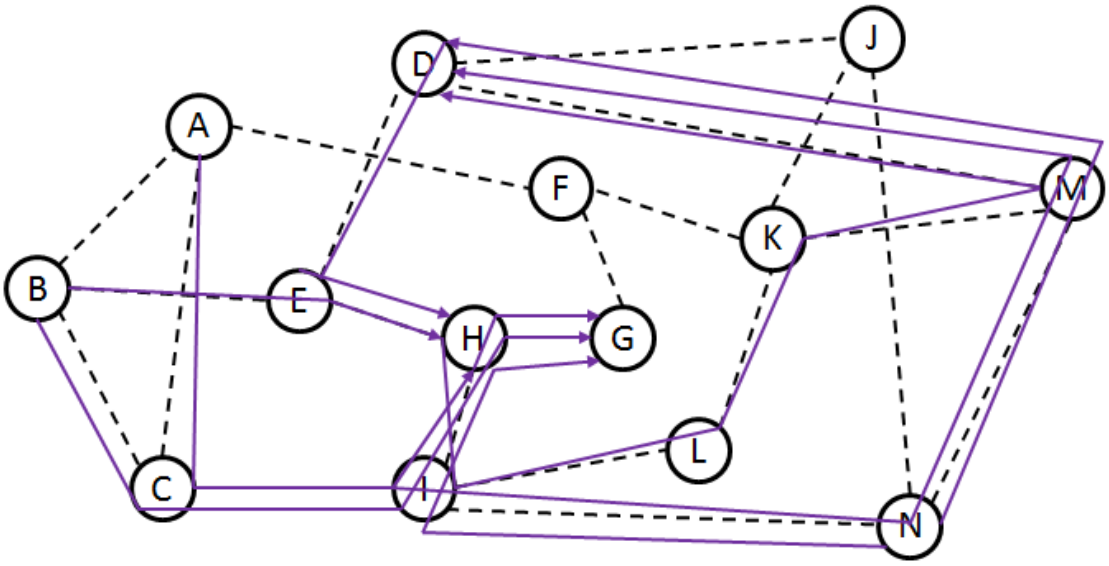

図 4.3.6(c)：グループ 3 に関する信頼性重視のコンテンツ配信経路

図 4.3.7(a)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における効率性重視のコンテンツ配信経路の中のグループ 1 のみの経路を示したものである．この配信経路から配信サーバ A から配信されるピースが中継ノード E でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．また，配信サーバ B から配信されるピースが中継ノード E，H でマルチキャスト転送され，異なる配信先ノード D，G，H に配信されていることが分かる．更に，配信サーバ N から配信されるピースが中継ノード H でマルチキャスト転送され，異なる配信先ノード G，H に配信されていることが分かる．

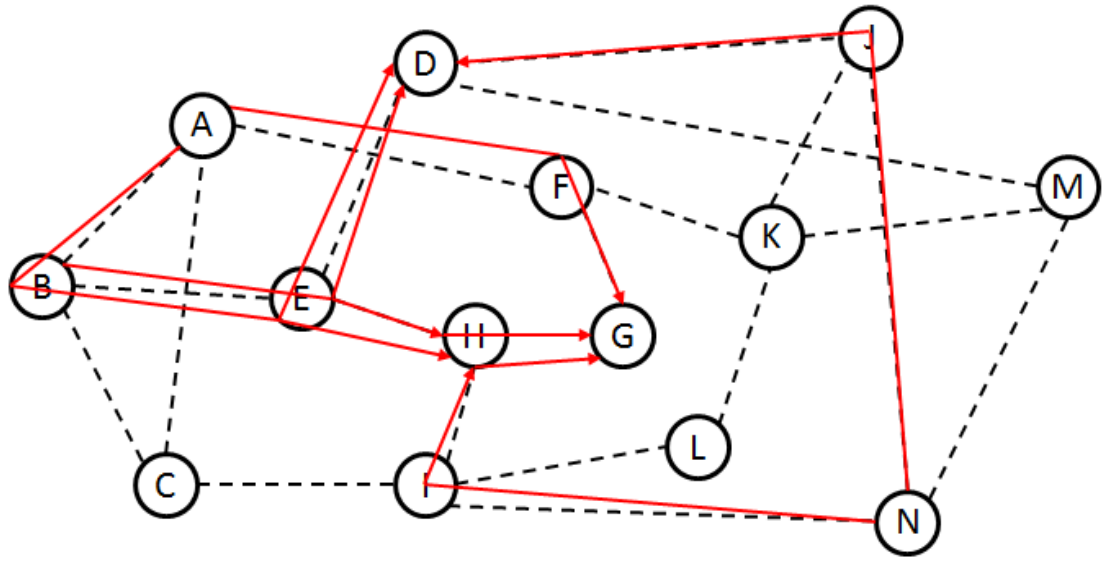

図 4.3.7(a)：グループ 1 に関する効率性重視のコンテンツ配信経路

図 4.3.7(b)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における効率性重視のコンテンツ配信経路の中のグループ 2 のみの経路を示したものである．この配信経路から

配信サーバ A から配信されるピースが中継ノード E でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．また配信サーバ B から配信されるピースが中継ノード E，H でマルチキャスト転送され，異なる配信先ノード D，G，H に配信されていることが分かる．更に，配信サーバ N から配信されるピースが中継ノード H でマルチキャスト転送され，異なる配信先ノード G，H に配信されていることが分かる．

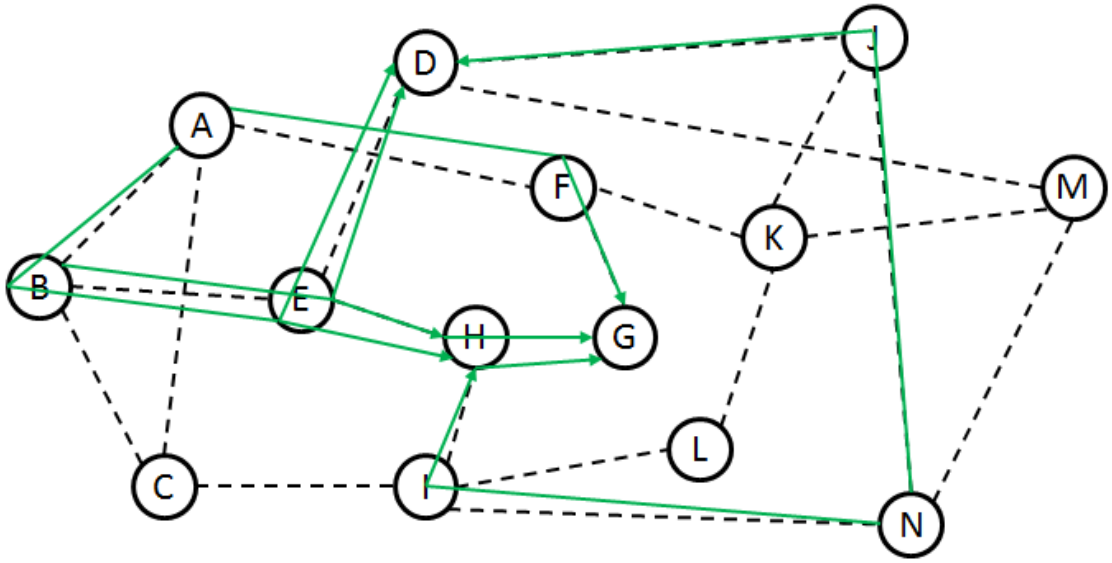

図 4.3.7(b)：グループ 2 に関する効率性重視のコンテンツ配信経路

図 4.3.7(c)は，グループ数 G=3 についての計算順序 1 とグループ化 2 における効率性重視のコンテンツ配信経路の中のグループ 3 のみの経路を示したものである．この配信経路から配信サーバ A から配信されるピースが中継ノード E でマルチキャスト転送され，異なる配信先ノード D，H に配信されていることが分かる．また配信サーバ B から配信されるピースが中継ノード E，H でマルチキャスト転送され，異なる配信先ノード D，G，H に配信されていることが分かる．更に，配信サーバ N から配信されるピースが中継ノード H でマルチキャスト転送され，異なる配信先ノード G，H に配信されていることが分かる．

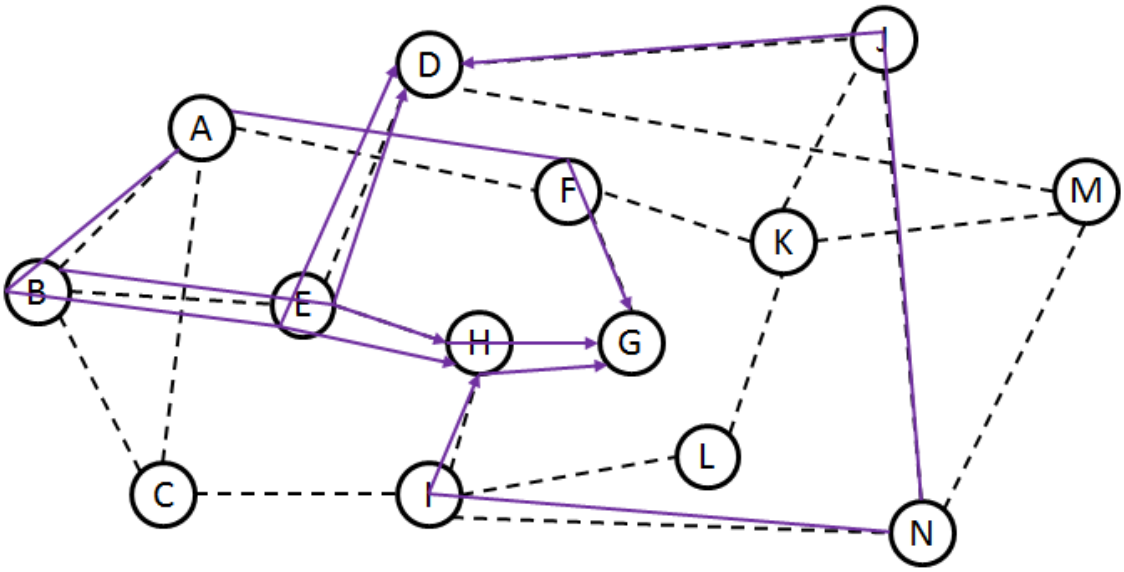

図 4.3.7(c)：グループ 3 に関する効率性重視のコンテンツ配信経路

図 4.3.2～4.3.7 より，信頼性重視のコンテンツ配信経路の場合，同一グループに含まれるピースは重複した配信経路によって転送され，異なるグループに含まれるピースは異なる配信経路によって転送される傾向になる．従って，グループ化 1 の場合には、各配信サーバからの配信経路は，各配信先ノードまでの同一の最小ホップ数経路となる．逆に，グループ化 2 の場合には，各配信サーバからの配信経路は，各配信先ノードまでのリンク独立な経路となる．以上より，信頼性重視のコンテンツ配信経路の場合は，グループ化 1 によって，各配信経路のホップ数が減少し，信頼性および効率性が向上する．

一方，効率性重視のコンテンツ配信経路の場合，グループ化 1 では，同一グループに含まれるピースの配信サーバが同一となるため，ネットワーク符号化が適用される可能性は低い．逆に，グループ化 2 の場合には，同一グループに含まれる異なるピースの異なる配信先ノードへの配信経路が途中で交差する可能性が高くなり，ネットワーク符号化の適用が促進される．従って，効率性重視のコンテンツ配信経路の場合，グループ化 2 によって，効率性は向上するが，信頼性は低下する．

4.3.2　実規模ランダムネットワークでの評価結果

ノード数 100 のランダムネットワークにおいて，配信サーバと配信先ノードの数や位置，閾値 K の値が異なる 5 つのケースについて評価し，その平均値を出した結果を表 4.3.8～4.4 に示す．

表 4.3.8 は，配信サーバと配信先ノードが各 3 つずつあり，N=9 及び K=6 の条件での結果である．複数の配信先は，コンテンツを 3 つの配信先ノードに同時配信した場合の結果を示し，個別の配信先は，個別の配信先ノードに対してのみコンテンツを配信した結果をまとめたものである．

次に表 4.3.9 は，配信サーバと配信先ノードが各 4 つずつあり，N=16 及び K=12 の条件での結果である．複数の配信先は，コンテンツを 4 つの配信先ノードに同時配信した場合の結果を示し，個別の配信先は，個別の配信先ノードに対してのみコンテンツを配信した結果をまとめたものである．

最後に表 4.4 は，配信サーバと配信先ノードが各 4 つずつあり，N=16 及び K=8 の条件での結果である．複数の配信先は，コンテンツを 4 つの配信先ノードに同時配信した場合の結果を示し，個別の配信先は個別の配信先ノードに対してのみコンテンツを配信した結果をまとめたものである．更に，2 つの配信先は，2 つの配信先ノード(前半の 2 ノードと後半の 2 ノード)に分けてコンテンツを同時配信した結果をまとめたものである．また，各ケースの損失率を計算する際，1 重リンク障害において損失率 0 である場合は，2 重リンク障害についての損失率を求めた．尚，下表の評価結果では，1 重リンク障害で損失率が 0 でない場合も 2 重リンク障害の損失率が示されているが，これは 1 重リンク障害で損失率が 0 であるケースが含まれるためである．リンク帯域と損失率に関しては，4.2.1 節と 4.2.2 節で定義した計算方法のもとで扱うとする．

表 4.3.8：配信サーバと配信先ノードが 3 つ(N=9，K=6)の評価結果

配信先ノード	設定条件	信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	84.6	8.866	73.2	9.934
	G=1，計算順序2	84.6	8.866	73.2	9.934
	G=3，計算順序1，グループ化1	100.8	1重:0 2重:50.6	76.8	1.268
	G=3，計算順序1，グループ化2	110.6	1重:1.066 2重:323	73.2	9.934
	G=3，計算順序2，グループ化1	100.8	1重:0 2重:50.6	76.8	1.268
	G=3，計算順序2，グループ化2	108.4	2	73.2	9.934
	G=9，計算順序1	124	1重:0 2重:79.26	76.8	1.268
	G=9，計算順序2	115.6	1重:0 2重:73.2	76.8	1.268
個別の配信先	G=9，計算順序1	134.4	1重:0 2重:79.27	96.6	1重:1.4 2重:30.5
	G=9，計算順序2	127.4	1重:0 2重:73.4	96.6	1重:1.4 2重:30.5

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.9：配信サーバと配信先ノードが 4 つ(N=16，K=12)の評価結果

配信先ノード		信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	172	10.3	139.2	11.65
	G=1，計算順序2	172.4	11	139.2	11.65
	G=2，計算順序1，グループ化1	183.2	12.25	144	11.65
	G=2，計算順序1，グループ化2	192.4	16.4	139.2	11.65
	G=2，計算順序2，グループ化1	178.6	15.6	144	11.65
	G=2，計算順序2，グループ化2	181.4	24.55	139.2	11.65
	G=4，計算順序1，グループ化1	201.6	1	147.2	2.4
	G=4，計算順序1，グループ化2	254.8	4.35	139.2	11.65
	G=4，計算順序2，グループ化1	200.2	2	147.2	2.4
	G=4，計算順序2，グループ化2	254.6	3.3	139.2	11.65
	G=8，計算順序1，グループ化1	254.8	1.65	145.6	2.4
	G=8，計算順序1，グループ化2	283.4	2.6	140.8	11.65
	G=8，計算順序2，グループ化1	232	2.55	147.2	2.4
	G=8，計算順序2，グループ化2	273.2	2.45	144	11.65
	G=16，計算順序1	264.2	2.05	147.2	2.4
	G=16，計算順序2	239.8	1.95	147.2	2.4
個別の配信先	G=16，計算順序1	304	2.1	216	2.4
	G=16，計算順序2	283	1.95	216	2.4

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.4：配信サーバと配信先ノードが 4 つ(N=16，K=8)の評価結果

配信先ノード		信頼性		効率性	
		リンク帯域	損失率	リンク帯域	損失率
複数の配信先	G=1，計算順序1	172.8	10.5	140	11.6
	G=1，計算順序2	172.8	11.1	140	11.6
	G=2，計算順序1，グループ化1	196.8	1重:0 2重:37.55	144	1.8
	G=2，計算順序1，グループ化2	218.8	1重:0.2 2重:108.81	140	11.6
	G=2，計算順序2，グループ化1	196	1重:0 2重:39.7	144	1.8
	G=2，計算順序2，グループ化2	220.4	1重:0.4 2重:129.38	140	11.6
	G=4，計算順序1，グループ化1	211.2	1重:0 2重:6.7	147.2	0.8
	G=4，計算順序1，グループ化2	252.2	1重:0.45 2重:102.5	140	11.6
	G=4，計算順序2，グループ化1	204.2	1重:0.05 2重:15.75	147.2	0.8
	G=4，計算順序2，グループ化2	259.4	1重:0.55 2重:77.38	140	11.6
	G=8，計算順序1，グループ化1	236	1重:0 2重:4.65	147.2	0.8
	G=8，計算順序1，グループ化2	234.2	1.55	141.6	1.6
	G=8，計算順序2，グループ化1	214.4	1重:0.1 2重:32.44	147.2	0.8
	G=8，計算順序2，グループ化2	264.4	1重:0 2重:35.7	144	1.8
	G=16，計算順序1	233.8	1重:0 2重:6.95	147.2	0.8
	G=16，計算順序2	221	1重:0 2重:5.55	147.2	0.8
個別の配信先	G=16，計算順序1	272.6	1重:0 2重:6.95	215.2	1重:0.667 2重:12.83
	G=16，計算順序2	266.8	1重:0 2重:5.55	215.2	1重:0.667 2重:12.83
2つの配信先	G=1，計算順序1	193	10.5	163.2	11.05
	G=1，計算順序2	193.2	11.1	163.2	11.05
	G=16，計算順序1	253.4	1重:0 2重:6.95	169.6	0.75
	G=16，計算順序2	244	1重:0 2重:5.55	169.6	0.75

(損失率は 1 重リンク障害確率や 2 重リンク障害確率の積をとる値)

表 4.3.8～4.4 の結果から，実規模なネットワークでも，閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに個別に配信する場合と比較して，複数の配信先ノードに同時配信することにより，所要リンク帯域容量が減少し，効率的なコンテンツ配信を実現できる．また，提案コンテンツ配信法では，グループ数の増加に伴い，信頼性が向上するが効率性が低下する．更に，信頼性を重視した配信経路計算と効率性を重視した配信経路計算を比較する

と，信頼性を重視した配信経路計算では，所要リンク帯域容量が増加するが，ピースの損失率が低くなることが分かる．一方，効率性を重視した配信経路計算では，所要リンク帯域容量が小さくなるがピースの損失率が大きくなることが分かる．

更にグループ分割数の変化により，所要リンク帯域容量やピースの損失率が大きく変化することも分かる．例えば，信頼性重視の配信経路計算において，G=1 や G=2 の時は，単一リンク障害のみで元のコンテンツを復元できない可能性が高くなることが分かる．逆にグループ数が G=4 や G=8，G=16 の時は，単一リンク障害によって元のコンテンツが復元できなくなる状況を回避できる可能性が高くなることが分かる．また，信頼性重視のコンテンツ配信経路の場合は，グループ化 1 によって，各配信経路のホップ数が減少し，信頼性及び効率性が向上する．更に，効率性を重視した配信経路計算において，グループ数を G=2 や G=4 や G=8 に分割した時，異なる配信サーバに保持されているピースを優先的にグループ化することにより，ネットワーク符号化が促進されて，ピースの損失率が増加する反面，所要リンク帯域容量が小さくなることが分かる．

以上より，例えば信頼性に対する要求条件として，損失率が 2 重リンク障害確率×10.0 以下であるとした時, グループ数を G=4 に設定して, 信頼性重視の配信経路計算と計算順序 1, グループ化 1 を採用することにより，信頼性に対する要求条件を満足しつつ，最も効率的なコンテンツ配信を実現できることが分かった．従って，提案コンテンツ配信法を用いることで，グループ数や配信経路の計算順序，ピース群のグループ化の条件を変えることにより，高信頼かつ高効率なコンテンツ配信を実現できる．尚，実規模なネットワークでもコンテンツ配信経路の計算は，ダイクストラ法の適用によって高速に行うことが可能である．

4.3.3 経路算出及び性能評価における所要計算時間

各評価対象ネットワークにおける提案コンテンツ配信経路計算法を用いた経路算出及び性能評価における所要計算時間は以下の表 4.4.1 の通りである．

表 4.4.1：経路算出及び性能評価の所要計算時間

NSF ネットワーク (N=9 , K=6)	実規模ランダムネットワーク (N=16 , K=12)	実規模ランダムネットワーク (N=16 , K=8)
約 5 分	約 10 分	約 35 分

また，様々なネットワークの経路算出における予想計算量は，ネットワーク規模，閾値秘密分散保持されたコンテンツを構成するピース数，配信先ノード数，配信サーバ群から各配信先ノードに至るリンク独立な経路の最大数に依存すると考えられる．ここで，ネットワークのリンク数を L，ノード数を V とし，ピース数を N，配信先ノード数を D，リンク独立な経路の最大数を m とする．リンクコストを更新する際，当該リンクを含む多重リンク障害を想定する計算量は，$O(L^{m-1})$で表されるため，全てのリンクコストを更新する計算量は$O(L^{m})$となる．一方，ダイクストラ法による計算量は$O(L+V)\log V$で表される．つまり，ネットワークのノード数とリンク数が同

じオーダーであるならば，経路算出において予想される計算量は式(23)となる．

$$O(N \times D \times L(L^{m-1} + \log L)) \qquad (23)$$

本評価と同様に，配信サーバ群から各配信先ノードに至るリンク独立な経路の最大数を m=3 とした場合，式(24)として表される．

$$O(N \times D \times L^3) \qquad (24)$$

ただし，logL は L の値が増加するにつれて一定の値に近づくため無視できるものとする．以上より，配信サーバ群から各配信先ノードに至るリンク独立な経路の最大数が 3 である場合，所要計算時間は，ネットワーク規模の 3 乗に比例して増加すると予想される．

5. 結論

本論文では，複数の配信サーバに(K,N)閾値秘密分散保持されたコンテンツを複数の配信先ノードに同時配信するコンテンツ配信法を提案した．複数の配信先ノードに同時配信することで，コンテンツ配信のタイミングが遅くなる恐れがあるが，ネットワーク符号化の適用によって，コンテンツ配信に必要なリンク帯域の有効利用が図れる．一方，ネットワーク符号化の適用は，リンク障害に起因する 1 つのピースの損失によって，配信先ノードにおいて複数のピースのネットワーク復号化ができなくなる可能性を招き，リソース利用効率は向上するが，コンテンツ配信の信頼性は低下する恐れがある．そこで，1 つのコンテンツを構成するピース群を複数のグループに分類し，ネットワーク符号化を同一グループに属するピースに対してのみ適用する方法を提案した．

提案コンテンツ配信法の性能評価を行うためには，コンテンツ配信経路を具体的に算出する必要がある．コンテンツ配信経路を算出するためには，制約条件の下で最適化を図る整数計画法モデルを用いた最適経路計算法が有用な方法である．しかし，整数計画法モデルを実用的な規模のネットワークに対して適用すると，計算資源の制約から短時間でコンテンツ配信経路を算出することが困難である．この問題を解決する方法として，リンクコストを調整しつつ，最小コスト経路の探索アルゴリズムであるダイクストラ法を用いて，各配信先ノードに至る N 本の配信経路を逐次的に計算する方法を提案した．つまり，欲張り法の考え方に基づき，新たな配信経路を逐次的に算出する際に，N－K＋1 本以上の配信経路が障害となる確率を極力増加させないようにリンクコストを更新して，最小コスト経路計算を行う方法を提案した．

評価結果から，閾値秘密分散保持されたコンテンツを 1 つの配信先ノードに個別に配信する場合と比較して，複数の配信先ノードに同時配信することにより，所要リンク帯域が減少し，効率的なコンテンツ配信を実現できることが判明した．また，提案コンテンツ配信法においては，ピース群を分類するグループ数の増加に伴い，リンク障害に対する信頼性は向上するが，リンク帯域利用効率は低下することが判明した．更に，提案コンテンツ配信法においては，配信経路の計算順序やピース群のグループ化の条件を変えることで，所要リンク帯域やピースの損失率が変化する．信頼性を重視した配信経路計算法と効率性を重視した配信経路計算法を比較すると，同一条件の下でも，信頼性重視の配信経路計算では，所要リンク帯域が増加するが，ピースの損失率が低くなり，効率性重視の配信経路計算では，所要リンク帯域は小さくなるが，ピースの損失率が大きくなる．

以上より，提案コンテンツ配信法において，ピース群のグループ数，配信経路の計算順序，ピース群のグループ化の条件を適切に設定することで，高信頼かつ高効率なコンテンツ配信を実現できる．

謝辞

本研究を進めるにあたり，ご指導及びご協力頂いた，電気通信大学大学院情報システム学研究科情報ネットワークシステム学専攻ネットワークコンピューティング学講座の荻野長生客員准教授，吉永努教授，樫木勘四郎客員教授に心より感謝致します.

参考文献

[1] A.Sharmir , ”How to share a secret , ” Communications of the ACM , vol.22 , no.11 , pp.612-613 , Nov.1979

[2] Wenjing Lou , Wei Liu , and Yuguang Fang , “SPREAD : Enhancing Data Confidentiality in Mobile Ad Hoc Networks , “ Proc. of IEEE INFOCOM 2004 , 2004

[3] Amitabha Bagchi , Amitabh Chaudhary , Michael T. Goodrich , and Shouhuai Xu , “Constructing Disjoint Paths for Secure Communication , “ Springer Lecture Notes in Computer Science , Vol.2848 , pp.181-195 , 2003

[4] N.Ogino , T.Omi , and H.Nakamura：“ Route Computation method for secure delivery of secret shared content ” , IEICE Trans , Vol . E95-B , No.11 , pp.3456-3463(2012.11).

[5] Sushant Jain , Michael Demmer , Rabin Patra , and Kevin Fall , “Using Redundancy to Cope with Failures in a Delay Tolerant Network ,” Proc. of ACM SIGCOMM’05 , pp.109-120 , 2005

[6] 福島雅夫 , “数理計画入門” , 朝倉書店 , 1996.

[7] 柳浦睦憲 , 茨木俊秀 , “組合せ最適化－メタ戦略を中心として－” , 経営科学のニューフロンティア 2 , 朝倉書店 , 2001

[8] 高妻宜央 , 荻野長生 , ”閾値秘密分散保持されたコンテンツの高信頼配信経路計算法” , 平成 24 年度修士論文

[9] 中村勇勝 , 荻野長生 , “閾値秘密分散保持されたコンテンツの高信頼・高効率配信法” , 電子情報通信学会 ソサイエティ大会 , 2013