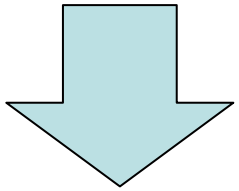
P2Pマルチキャストのための動的グループ鍵構成方法

Dynamic Group Key Construction for P2P Multicast

名城大学　理工学部　後藤　裕司

背景1

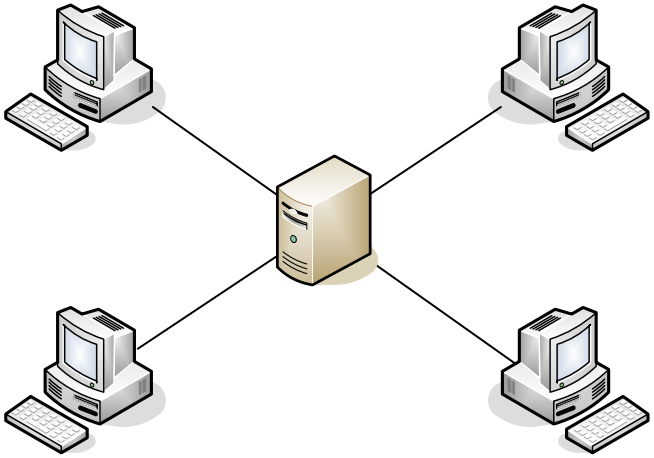
- ブロードバンド接続や有線や無線TV放送などのインターネットチャネルにおいて
  - 特定グループのユーザに対してだけコンテツを配信する技術が多くのビジネスやアプリケーションに必要



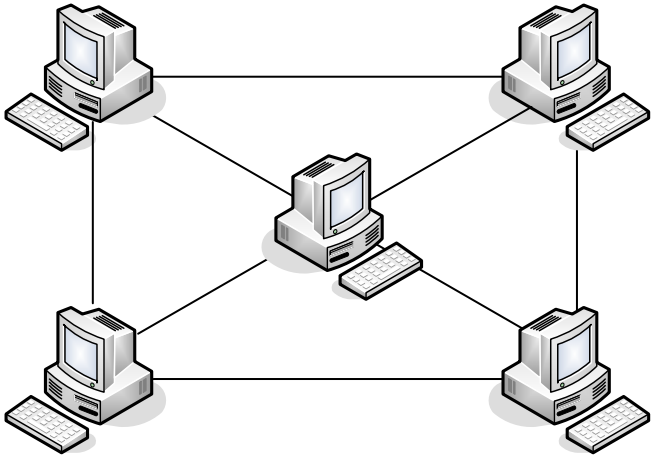
多数の受信者に対して効率的かつ安全に鍵の配送，更新，削除ができることが求められている

マルチキャストのセキュリティが研究されている

背景2



クライアント･サーバモデル



P2Pモデル

最近はゲーム機やTVなどもインターネット接続機能を持っている

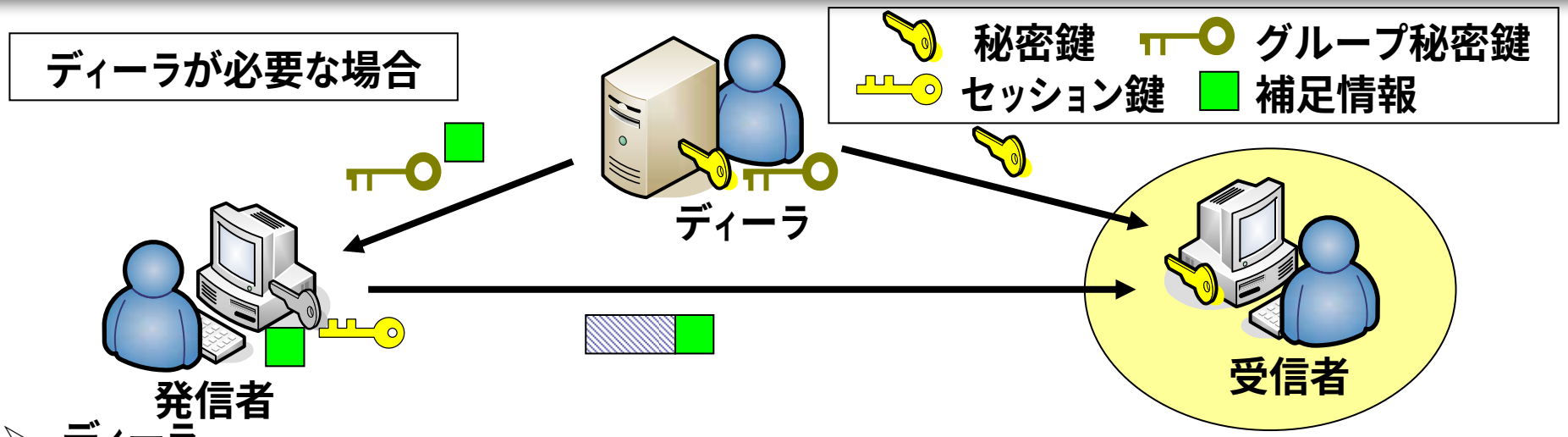
このような環境下では，マルチキャストのセキュリティを考えるとホスト同士の結託を不正とするような想定は成り立たない

P2Pに適した新しいシステムが必要となる

P2P環境下でのグループ鍵配信システムへの要件

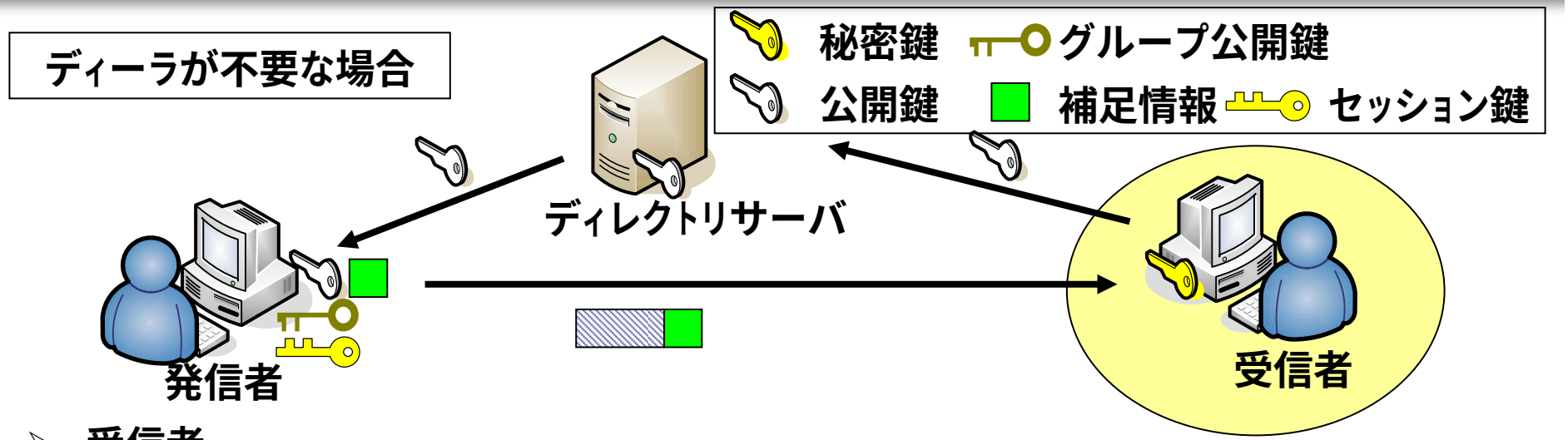
- 動的グループ鍵生成
  - メッセージ送信時に受信グループを任意に決められる
- 動的復号閾値生成
  - 指定した受信グループのうち，何人集まれば復号できるかの閾値をメッセージ送信時に決められる
- 協調復号
  - 受信グループは復号閾値で指定された人数が集まって初めてメッセージを協調復号できる
- 結託耐性
  - 受信グループ以外の者が何人共謀しても送信されたメッセージの復号や他のメンバの秘密鍵を知ることはできない
- 全体集合非依存性
  - グループ鍵は全体集合には依存しない

プロトコルの概要1



- ディーラ
  1. 送信者が指定したグループ集合と復号閾値mからメッセージ暗号化のためのグループ秘密鍵と補足情報を生成アルゴリズを使って生成し送信者に送付
- 発信者
  2. **セッション鍵 (共通鍵)** を生成し，**セッション鍵をグループ秘密鍵で暗号化**し，補足情報とともにメッセージヘッダに加える
  3. **メッセージをセッション鍵で暗号化**する
- 受信者
  4. メッセージ復号アルゴリズムを用いて，同一受信グループの他のメンバと協調することによってメッセージを復元する

プロトコルの概要2



- 受信者
  1. 秘密鍵を生成し，秘密鍵に対応する公開鍵をディレクトリサーバに登録
  6. メッセージ復号アルゴリズムを用いて，他のメンバと協調してメッセージを復元
- 発信者
  2. 送信したいグループ集合に対する公開鍵をディレクトリサーバから取得
  3. 公開鍵と復号閾値mを生成アルゴリズムでグループ公開鍵と補足情報を生成
  4. 乱数とセッション鍵を生成しElGamal暗号によってグループ公開鍵で暗号化
  5. 補足情報をメッセージヘッダとして，メッセージをセッション鍵で暗号化してマルチキャスト送信

ElGamal暗号

- **ElGamal暗号**
  - **公開鍵型の暗号方式**
  - Diffie-Hellman**鍵共有方式を暗号方式として利用できるように変形したものである**
  - **離散対数問題と呼ばれる数学の問題を応用した暗号で、平文と乱数と公開鍵から暗号文を作成し、秘密鍵で復号**

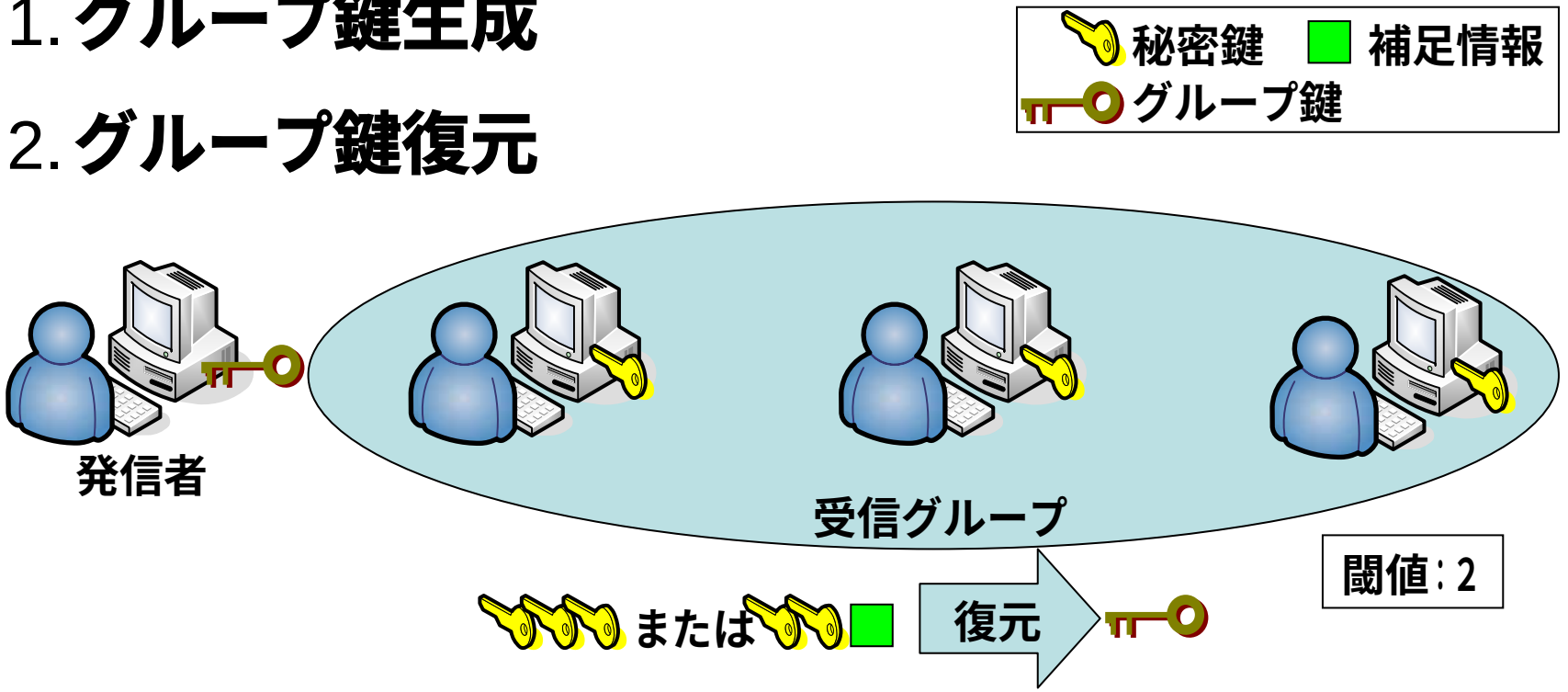
- **離散対数問題**
  - **公開鍵暗号方式の原理となる数学的性質のひとつ。**
  - **素数**p**と定数**q**が与えられたとき**

$$y=q^x \bmod p$$

をx**から計算することは容易だが、yからxを求めることは困難であること。**

セキュリティ要件1

1. **グループ鍵生成**
2. **グループ鍵復元**

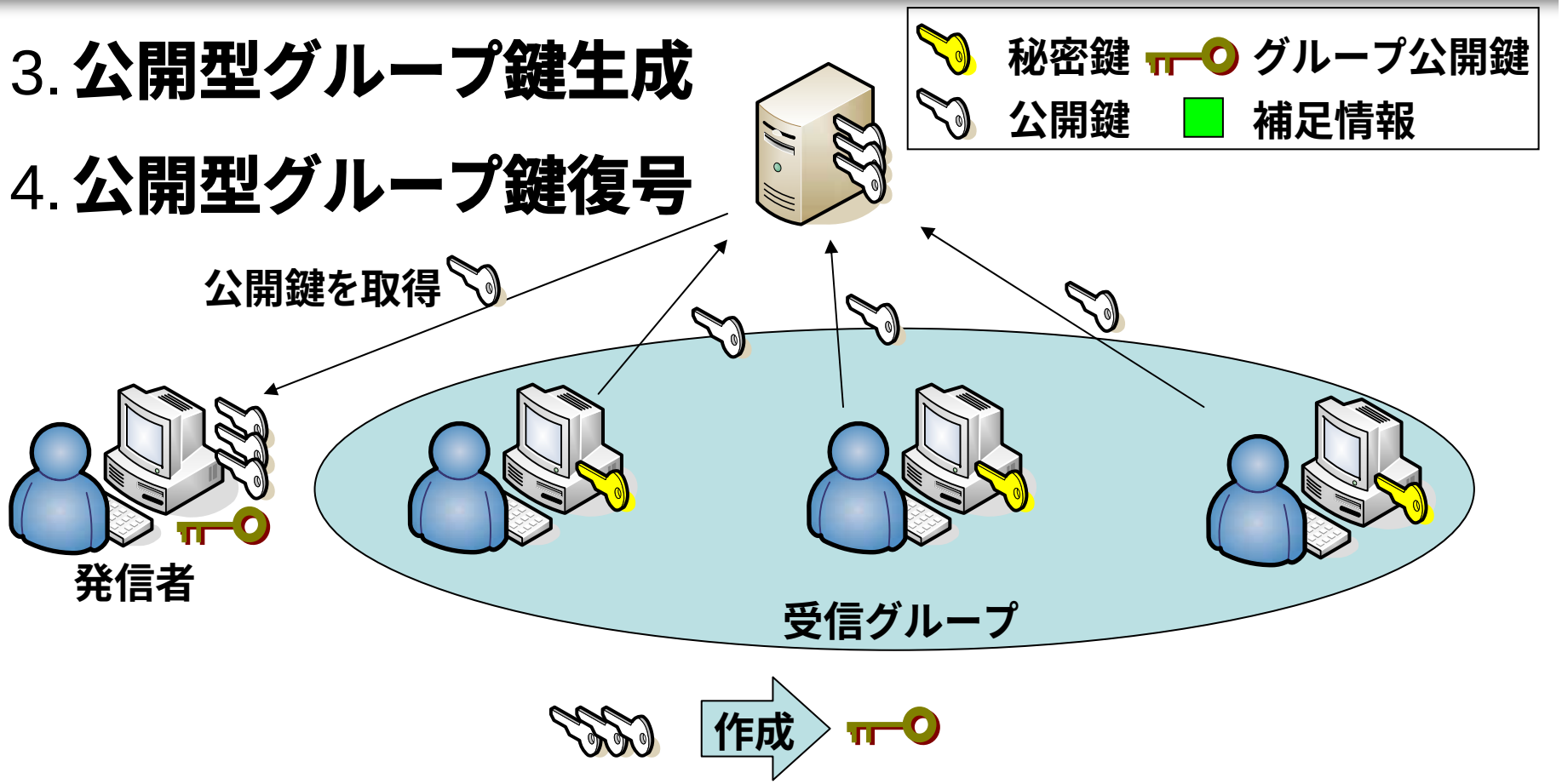


1. グループ鍵生成プロトコルで得られたグループ鍵は指定された受信グループの全ての秘密鍵またはそのうちのm個を補完する補足情報を持ちいらなければ復元できない
2. グループ鍵復号プロトコルは，補足情報を用いることによって，受信グループのメンバのうちm人の秘密鍵を用いることでグループ鍵を復元できる

セキュリティ要件2

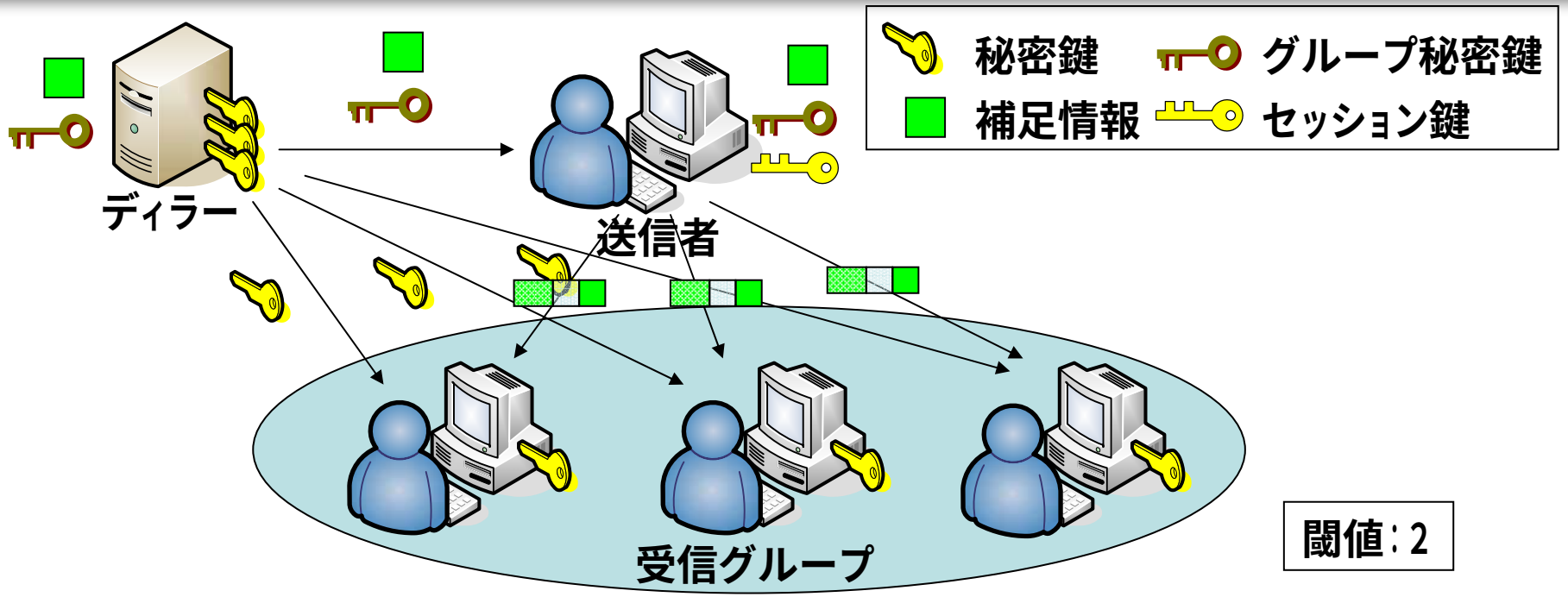
3. **公開型グループ鍵生成**

4. **公開型グループ鍵復号**



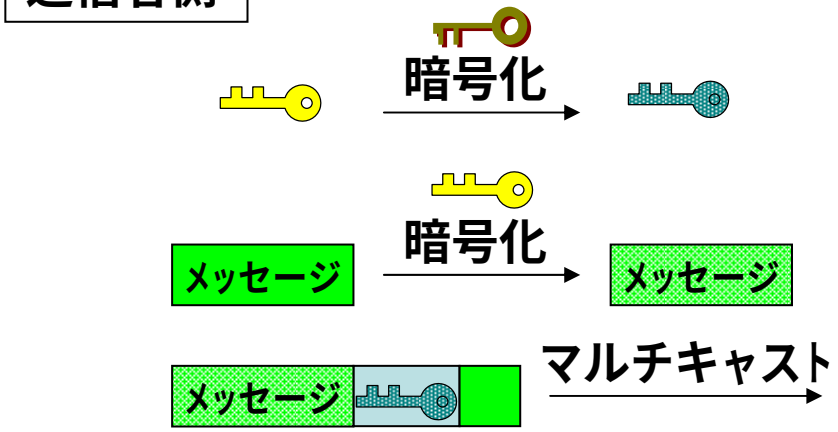
3. 公開鍵型グループ鍵生成プロトコルは受信グループのユーザの**公開情報のみ**から作られる
4. 公開鍵型復号プロトコルでは，受信グループのメンバはお互いに**秘密鍵を交換しなくても**，公開鍵型グループ鍵生成プロトコル**で暗号化されたメッセージを復号できる**

秘密鍵による動的グループ鍵構成法

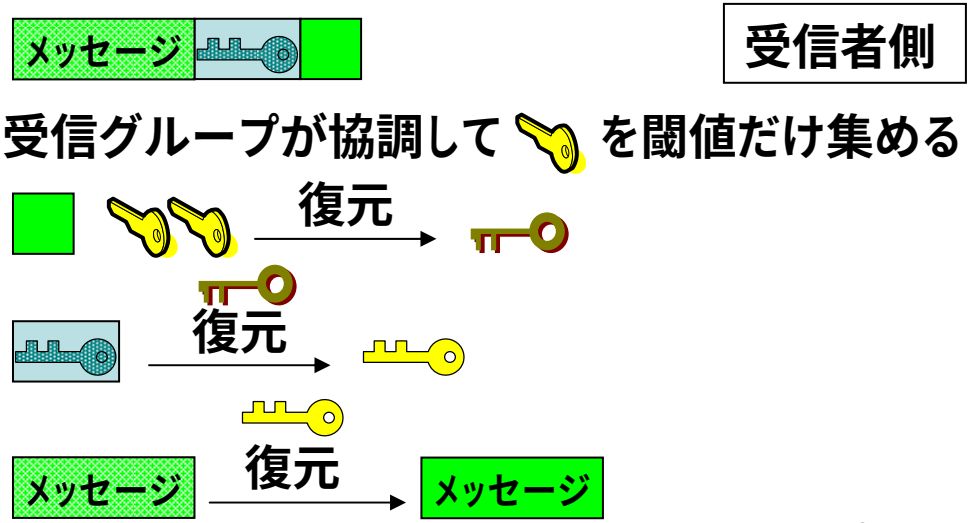


閾値：2

送信者側



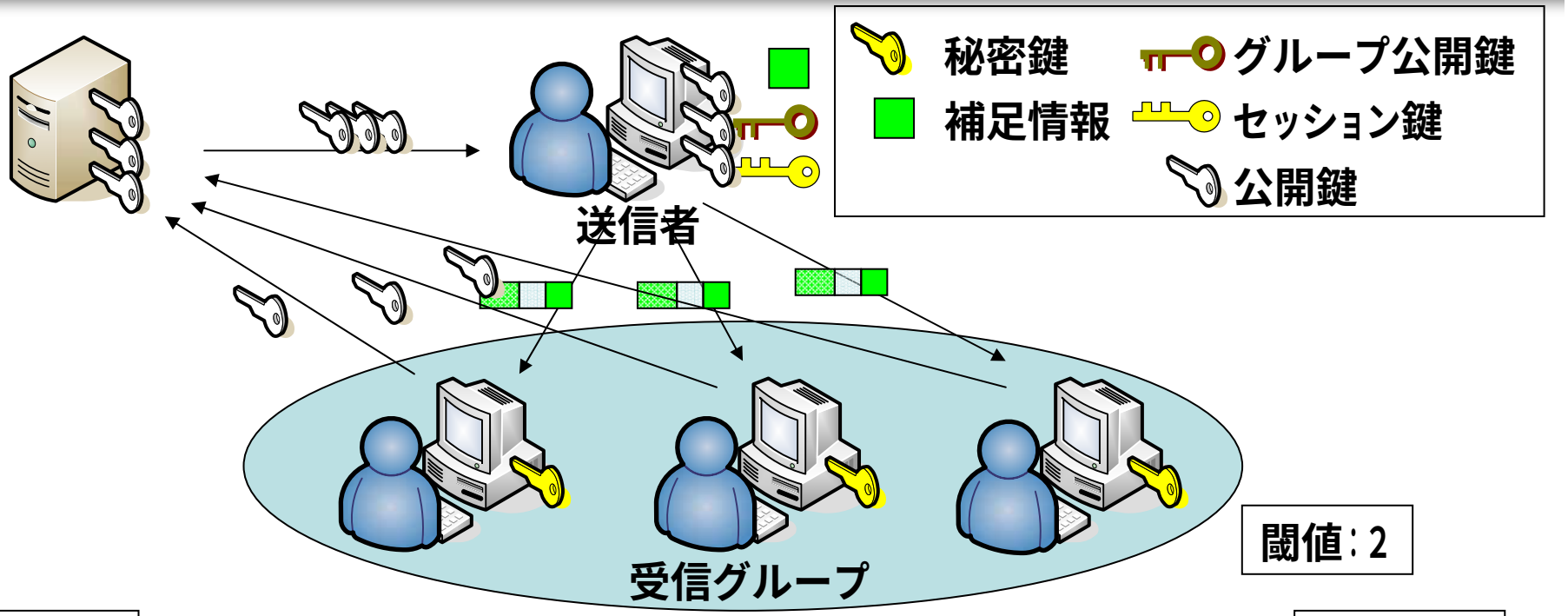
受信者側



セキュリティの考察1

- セキュリティ要件1,2を満たすが要件3,4は満たさない
  - グループ鍵はディーラによって作成される
  - 受信者同士での秘密鍵の交換が必要
    - 秘密鍵は1回限りの使い捨てになる

公開鍵による動的グループ鍵構成法



送信者側

ElGamal暗号

暗号化

メッセージ

メッセージ

マルチキャスト

メッセージ

受信者側

メッセージ

受信グループが協調して閾値だけ復号情報（閾値暗号）を集める

と復号情報で復元

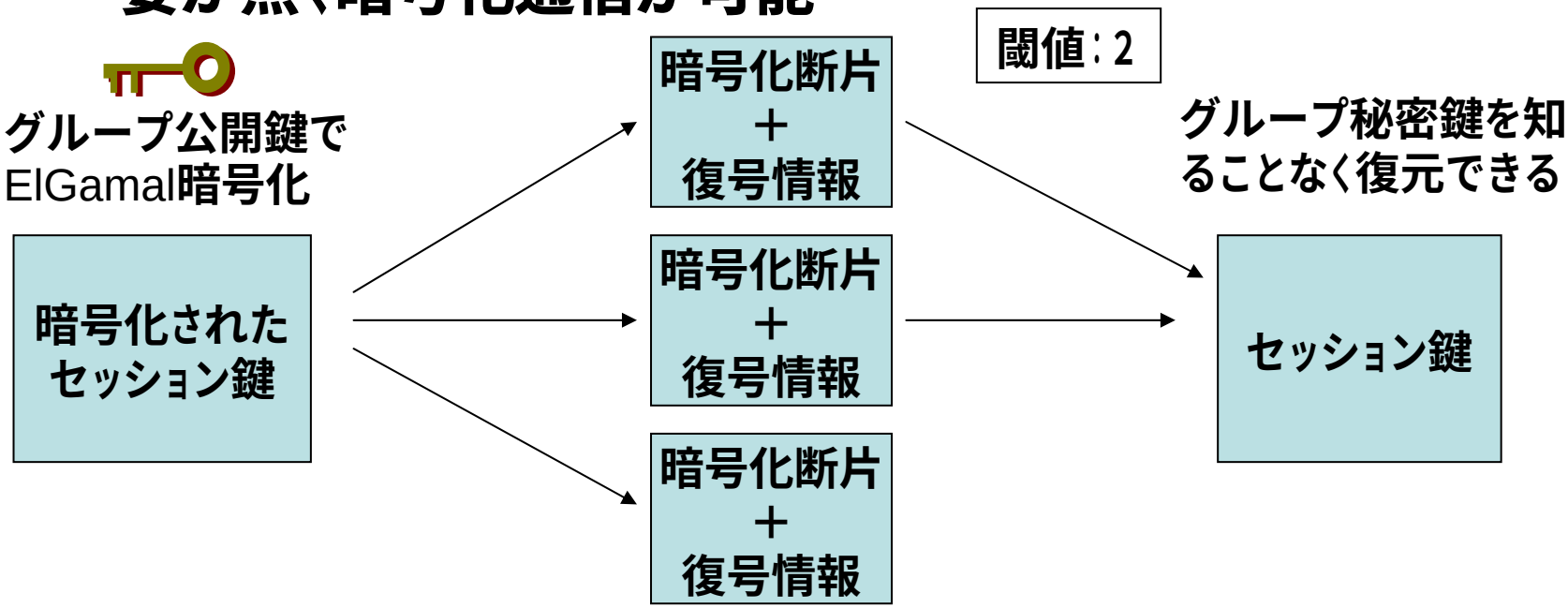
復元

メッセージ

メッセージ

閾値暗号を使うことによって

- 閾値暗号
  - 共通鍵方式や公開鍵方式と 異なり、暗号化断片に復号情報を埋め込むことで、事前に相手方との鍵の授受の必要が無く暗号化通信が可能



- 個々の復号情報だけでは復号できない
- 復号情報を閾値だけ集めるとセッション鍵を復元できる

セキュリティの考察2

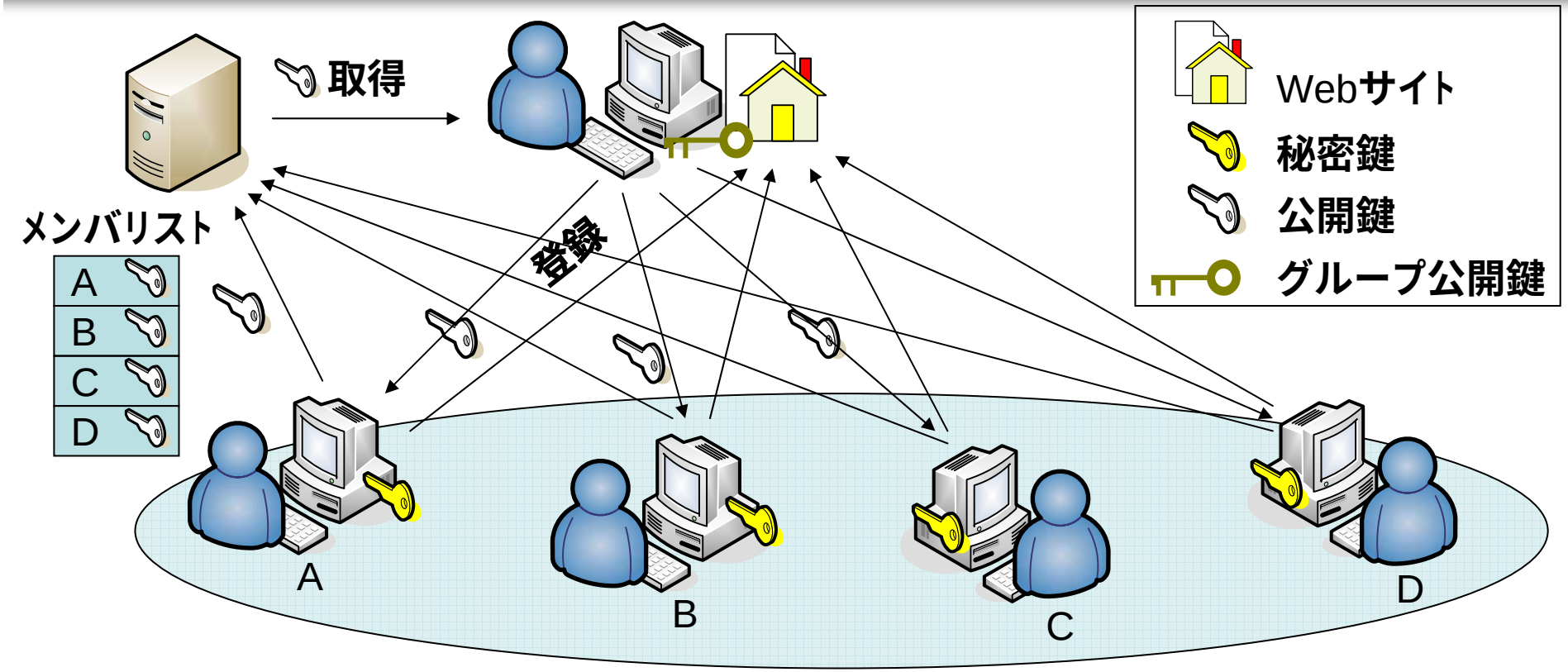
- セキュリティ要件を全てを満たす
  - セキュリティ要件3，4については，離散対数問題からそれぞれ満たされる
    - 秘密鍵を交換しなくてもメッセージを復号することができる

応用例

本システムを使用することによって

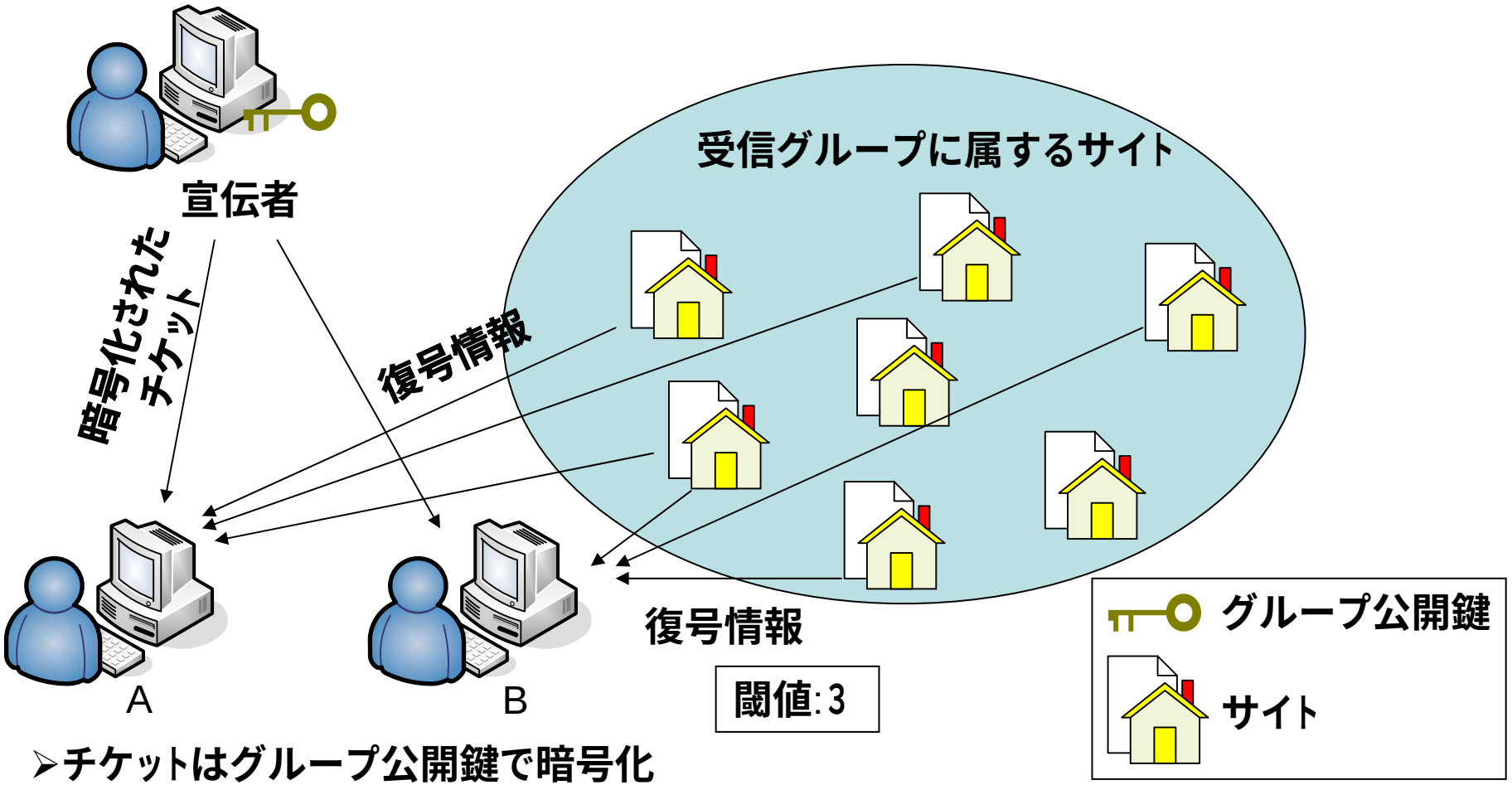
- コンテツ供給者の利点
  - 任意のサブセットを受信グループとして定義できる
  - グループのメンバだけが復号できるようなグループ暗号鍵が構成できる
  - TTP (第三者信頼機関) は必要ない
- コンテツ受信者の利点
  - 自分で自分の秘密鍵を生成できる
  - 公開鍵を公開するだけで，コンテツの受信者となれる
  - ネットワークに接続さえすれば受信者になれる

典型的なシナリオ



1. コンテツ供給者は自らのWebサイトをたて利用者を募る
2. 利用者はサイトに登録する
3. 自分で秘密鍵を生成し，それに対する公開鍵をメンバリストに登録する
4. コンテツ供給者はメンバリストに登録された公開鍵に基づいてグループ鍵を生成してコンテツを暗号化してマルチキャストする
5. 利用者はメンバリストを参照しながら他のメンバと協力してコンテツを復元

サーバー訪問メータリングシステム



- チケットはグループ公開鍵で暗号化
- 受信グループに属するサイトを訪問すると復号情報を得る
- 決められた閾値に達するとチケットが解読できる

まとめ

- P2Pマルチキャスト通信を目的としたグループ鍵構成法を提案
  - P2P環境下でのグループ鍵配信システムへの要件
  - 公開鍵による動的グループ鍵構成法
    - 公開情報のみで動的に受信グループや閾値が設定でき，鍵サイズは受信グループのサイズに依存しない
    - 閾値暗により秘密鍵を交換しない
- 本システムの応用例
  - 典型的なシナリオ
  - サーバー訪問メータリングシステム

おわり

補足：グループ秘密鍵の生成と復号

- **グループ鍵SGの生成法**
  - Lagrangeの補間法

$$f(x) = \sum_{i \in G_{id}} \lambda(x) si$$

$$\lambda i(x) = \prod_{j \in G_{id}, j \neq i} (x - j)(i - j)^{-1}$$

グループ鍵をSG＝f(0)とする

SG{Sg1,Sg2,…,Sgn}：**秘密鍵の集合**

Gid{g1,g2,…,gn}:**受信グループのID集合**

G’id{g’1,g’2,…,g’n}:**復号メンバの集合**

- **グループ鍵の復号**
  - **秘密鍵の集合と補足情報からLagrangeの補間法を用いて求める**

$$f'(x) = \sum_{i \in G'_{id} \cup \triangle} \lambda i(x) Si$$

$$\lambda i(x) = \prod_{j \in G'_{id} \cup \triangle, j \neq i} (x - j)(i - j)^{-1}$$

グループ鍵はSG＝f’(0)によって復元される

補足：グループ公開鍵の生成とセッション鍵の復号

- **グループ公開鍵y_Gの生成法**

$$y_G = \prod_{i \subset G_{id}} Yi^{\lambda i(0)} \pmod p$$

$$\lambda i(0) = \prod_{j \in G_{id}, j \neq i} (\delta_k - j)(i - j)^{-1}$$

y_G:グループ公開鍵
S_G:グループ秘密鍵
p,q:q|p-1を満たす大きな素数
g:有限体Z_p上の位数qの元
r:乱数

- **セッション鍵の直接復号とメッセージの復号**

ElGamal暗号 $ElG_{y_G}(K) = (g^r, Ky_G{}^r)$ を前半と後半をAとBに分ける

$(A, B) = (g^r, Ky_G{}^r)$ 各自が補足情報を用いることで以下のように A^{S_G}を計算

$$A^{S_G} = \prod_{i \in \triangle} y_i{}^{r\lambda i(0)} \prod_{i \in G'_{id}} A^{S_i \lambda i(0)} \pmod q$$

$$\lambda i(0) = \prod_{j \in G'_{id} \cup \triangle, j \neq i} (-j)(i - j)^{-1} \pmod p$$

ここで $y_G = g^{S_G}$ となっているので

$$\frac{B}{A^{S_G}} = \frac{Ky_G{}^r}{(g^r)^{S_G}} = K \pmod p$$

セッション鍵Kが復元でき，セッション鍵でメッセージを復元できる

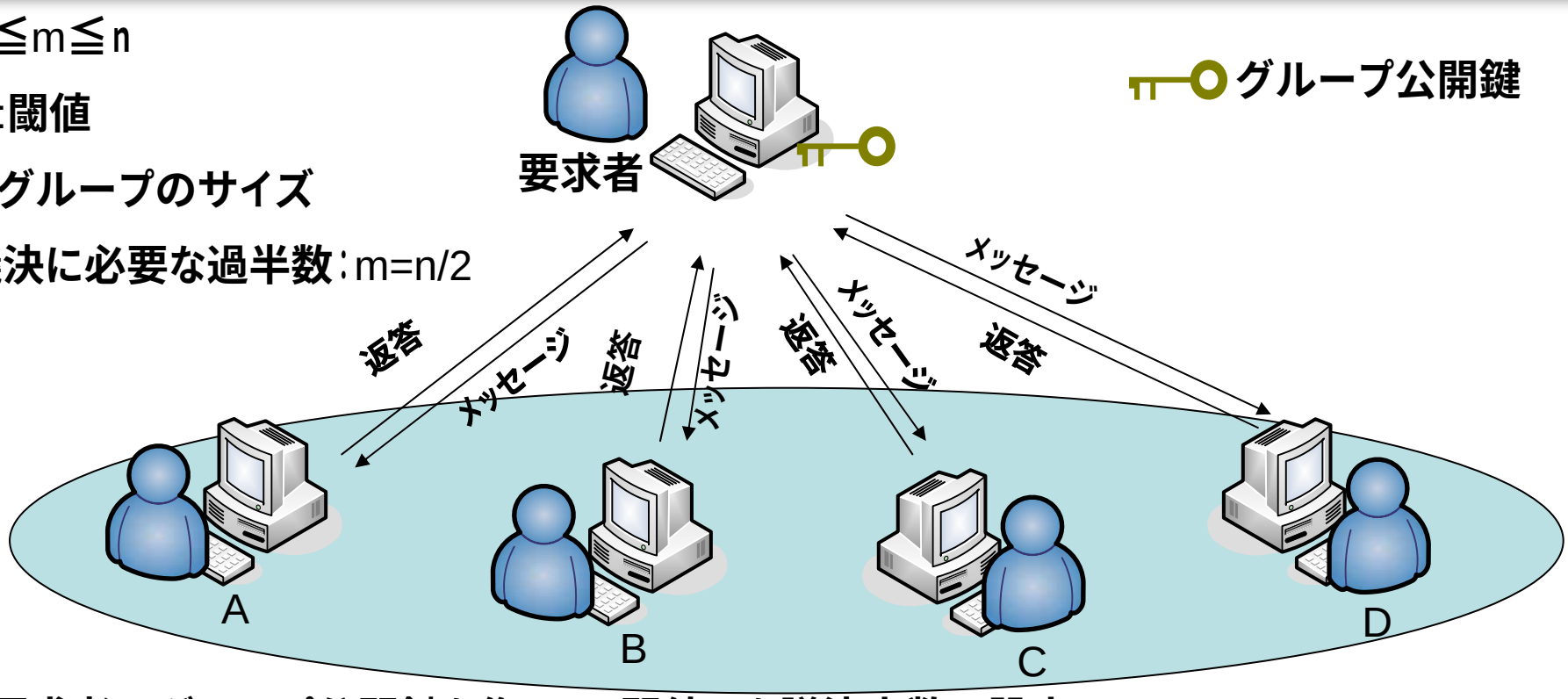
合議事項伝達システム

1≦m≦n

m:閾値

n:グループのサイズ

議決に必要な過半数：m=n/2



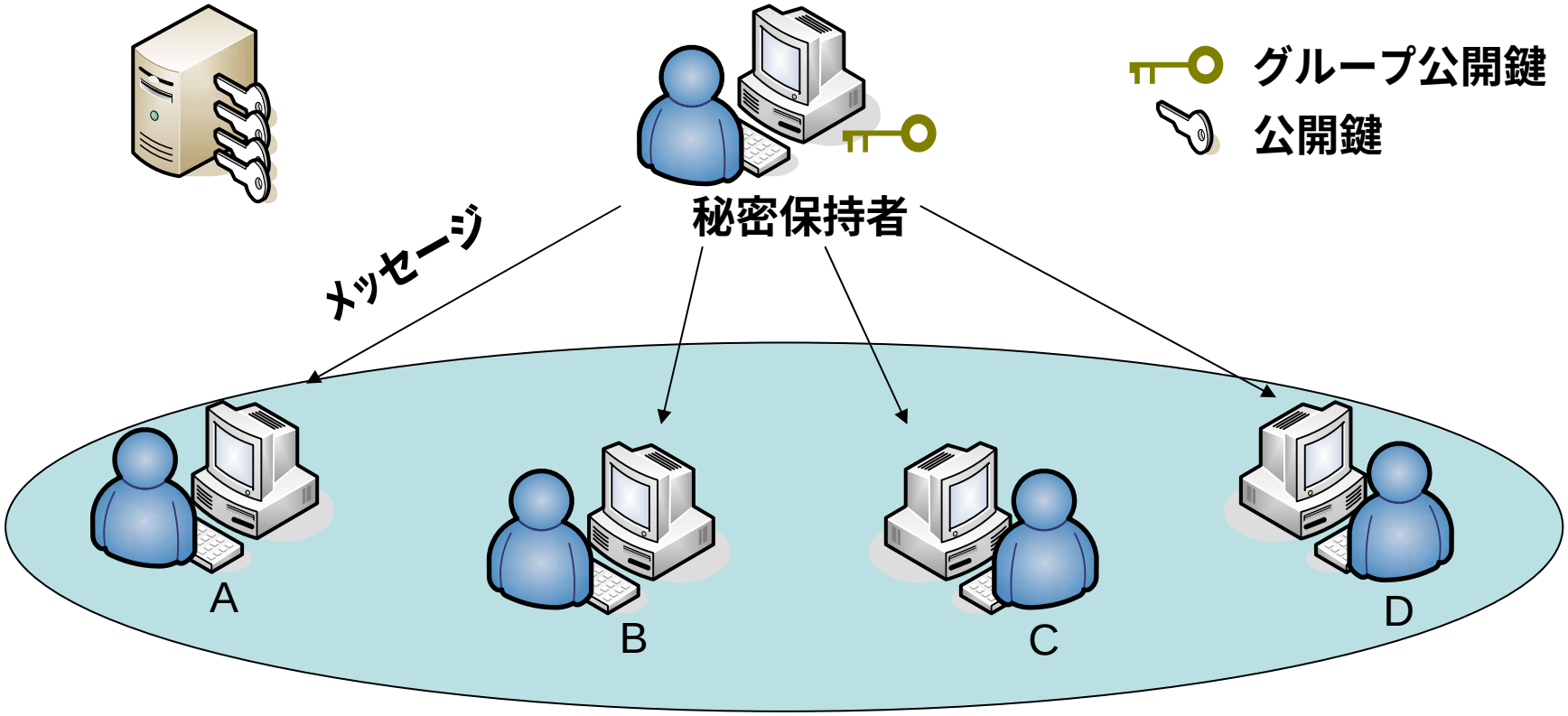
要求者はグループ公開鍵を作って，閾値mを議決定数に設定

グループ公開鍵でメッセージを暗号化してマルチキャストする

メッセージを復号するために閾値m以上のメンバが集まることが必要

議題が読めたということは議決定数の人数が集まったということ
返事である議決も有効なものと見なせる

任意のグループに対する秘密分散システム



1. 秘密分散者の公開鍵からグループ公開鍵を作る
2. グループ公開鍵で暗号化して送信
3. 閾値mを秘密復元に必要な最低人数を設定する
4. m人の分散値保持者が集まることによって復元できる

類似システムとの比較

m:閾値　n:グループのサイズ　k:不正者　k’:復号処理をしない欠席者の人数

	本システム	Broadcast Encryption	グループ暗号	動的閾値暗号処理
秘密鍵生成	ユーザ	TTP	ユーザ	ユーザ
グループ指定	送信者	TTP	固定	送信者
協調復号	m,n　可変	ー	m,n　固定	m,n　可変
結託閾値	ー	K	ー	ー
秘密鍵量	1	$k \log k \log n$	1	1
送信メッセージ量	1+k’ k’=n-m	$k^2 \log^2 k \log n$	1	n
復号メッセージ量	m^2	ー	m^2	m^2

- 動的に受信グループと閾値を選べ，送信メッセージが受信グループに依存しない
- 欠席者が受信グループのサイズに対して小さいときに有効

- **対称性**
  - P2Pのホストはクライアントとサーバの両方の機能を持つ
- **接続性**
  - アプリケーション層に新たなアドレス空間を定義することによって，IPにとらわれないホスト同士の接続を確保
  - モバイル環境下も想定しているので動的なホストの加入や離脱にも対応
- **状態依存性**
  - トランザクションの状態を保持したプロトコルを定義

- ホスト同士の協調動作への対応
  - ホスト機能の対称性およびホスト同士の接続性から，ホスト間の協調動作が普通に行われることが前提となる
- 動的な受信者集合への対応
  - ホスト間の接続性から，受信者集合は動的に変化する
- スケーラビリティへの対応
  - インターネットに接続されたホストを扱うためにはプロトコルはサイズに依存しないことが望まれる