社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－DBS－143 (88)
2007／7／4

RMXにおける電子メール送受信範囲管理方式の提案

原田 哲志† 慎 祥揆† 遠山 元道††

† 慶應義塾大学大学院 理工学研究科 開放環境科学専攻
†† 慶應義塾大学 理工学部 情報工学科
E-mail: †{hara,shin}@db.ics.keio.ac.jp, ††toyama@db.ics.keio.jp

あらまし 近年, 個人情報保護の社会的要請が高まっており, 企業内情報システムにおいても情報を保護する仕組みが必要となっている. 本稿ではメール配送システムRMXにおける情報漏えいの防止, 不要メールの防止を目的として利用者の情報に基づいてメールを送受信できる範囲を制御するシステムを提案する. RMXにおけるメール配信行為は送信者, 受信者, 送信時に利用する配送ルールで表現される. 提案方式では配信行為, つまりこれらの組み合わせに対して許可を設定する. このような送信許可ルールを複数記述することで複雑なメール配信管理を実現する.
キーワード RMX, 電子メール, 個人情報

Proposal of an E-mail transmission and reception range management method in RMX

Satoshi HARADA†, Sang-Gyu SHIN†, and Motomichi TOYAMA††

† School of Science for OPEN and Environmental Systems,
Faculty of Science and Technology, Keio University.
†† Department of Information and Computer Science, Faculty of Science and Technology,
Keio University
E-mail: †{hara,shin}@db.ics.keio.ac.jp, ††toyama@db.ics.keio.jp

Abstract In late years a social request of personal information protection rises. So in a company, infomation system need mechanism to keep secret informations. In this paper we aim to prevent information leakage and unnecessary mail in email delivery system RMX. We propose a system to controll the range a user can send an email based on user information. In RMX the transmission of an email is expressed by sender, receiver and delivery rule. We set permission for such delivery act describing a permission rule. We realize complicated email delivery management by describing several such permission rules.
Key words RMX, email, Personal Information

1. まえがき

電子メールは情報化社会において必須のツールであると言える. その一つの利用方法としてメーリングリストがあり, 複数の送信先にメールを送信する方法としてさまざまな組織で組織内のコミュニケーションに使用されている. その一方で情報漏洩事件が続発し, 情報セキュリティに関する注目度が高まっており, 電子メールを介した情報漏洩もその一つとして挙げられる. また, 電子メール保存の義務化の動きが進んでおり, 深刻さを増す情報管理状況に対応するためにも電子メールによる情報流出を防ぐことが重要となっている.

2. 関連研究

メールによる情報漏洩を防止する対策は大きく分けてメールの「保存」,「フィルタリング」,「暗号化」

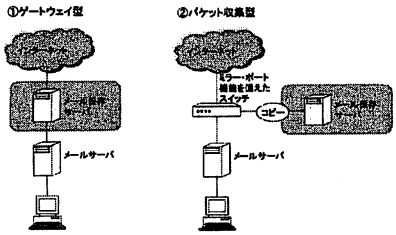

図 1 ゲートウェイ型とパケット収集型の概念図

が挙げられる. 以下でこれらについて説明する.

2.1 フィルタリング

フィルタリングはメールの検閲を行う技術である. これはメールの内容を検閲し, その際に引っ掛かった内容に基づき, 配送制御を行うというものである.

これはキーワード・マッチング [1] やスコアリング [2], [3] を使って実現される. これらの手法に基づき, 検閲に引っ掛かったメールに対して許可, 保留, 削除などの配送制御が行われる.

例えば研究所において研究内容の漏洩を防ぐために外部に送られるメールのフィルタリングを行い, 機密情報に関わる単語などが含まれている場合にはメールの送信を保留し, 手動で判断をするなどの利用が考えられる.

2.2 メールの保存

情報漏洩が発生した場合の監査証跡を確保するためにメールの保存は重要となる. また, 現在では電子メールは単にコミュニケーションのツールだけでなく契約, 決済といった, 商取引の文書としても利用され始めている. そうした中で, 電子メールは紙の文書と同じように法的な証拠として効力が認められつつある. 内部監査や, 訴訟の際の証拠とするためにも電子メールの保存体制が必要となっている.

メールの保存を行うための技術としては「ゲートウェイ型」と「パケット収集型」の 2 つの方法が一般的である. ゲートウェイ型は, ゲートウェイ自身を通過するメールをすべて保存するというものである. これに対してパケット収集型では, メールを含め, ネットワーク上を流れる任意のパケットを収集する. 図 1

2.3 暗 号 化

企業で使われるメールシステムの多くは, 暗号化技術として S/MIME (Secure Multipurpose In ternet Mail Extensions) [4] を実装している.S/MIME は公開鍵暗号方式を利用し, メール・メッセージを暗号化して送信する技術である. 暗号化した鍵と, それに対応する復号鍵がなければ, たとえそのメールを受け取っても読むことはできない. 第三者に読まれては困るような機密文書のメールでの利用が想定される. ただし, 現状では送信相手への鍵の受け渡し方法など事前の確認や準備の煩雑さなどからメール暗号化はそれほど普及していない.

また, 暗号化は監査とは相反する対策である. メールが暗号化されていると, 内容をチェックできないという問題がある. 安 健司らは, この問題を解決するために, メールサーバでチェック可能な方式を提案している [5].

3. 研 究 目 的

本研究では慶應大学遠山研究室で研究されている Rule-based e-Mail eXchange(RMX) [6], [7] の送信制限方式を拡張する. 送受信許可ルールを記述することで, より柔軟な送受信許可範囲制御を可能とする方式を提案する.

従来手法では二つの制限から一つを選択し利用者全体に適用するのに対し, 本研究では利用者の情報を利用し, 個々の利用者に応じた送受信許可を行う.

4. 提 案 手 法

4.1 RMX

Rule-based e-Mail eXchange(RMX) は遠山研究室が提案している電子メール配信方式である. 一般的にメール配信に利用されているメーリングリスト (ML) ではメーリングリストを代表するアドレスにメールが送信されるとメーリングリストに所属するメンバー全員に対してメールが配信される.

$$< ML\text{アドレス} >:=< ML\text{名} > @ < \text{ドメイン} >$$

メーリングリストではメンバーのメールアドレスの更新など管理者の作業負担が必要となる. 例えば大学でのメーリングリストの利用を考える. 学生がメールアドレスを変更した場合にはクラス, 研究室, プロジェクトなど所属する全てのメーリングリストでアドレスの変更を行わなければならない.

それに対して RMX では下記のような記述により複数の送信先を指定する.

$$< RMX\text{のメールアドレス} >:=$$
$$< \text{パラメータ} > @ < \text{配送ルール} > . < \text{ドメイン} >$$

RMX のメールアドレスは以上のように配送範囲記述部分とドメイン部分が"."の記号で区分されている. 配送範囲記述部は一つのパラメータの組み合わせで構成され, @記号によってパラメータと配送ルール名に分けられる. RMX はこのような配送範囲記述を受け取る. そして, 指定された配送ルールとそのパラメー

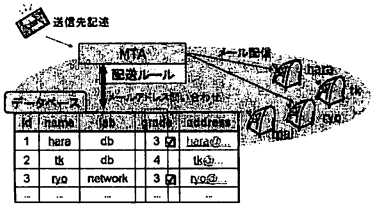

図 2 RMX におけるメール配信の流れ

タに基づきデータベースに問い合わせを行い実際の送信先アドレスを得る. 最終的に得られたメールアドレスに基づき配送が行われる. 図 2

RMX ではメール配信に必要な情報は全て利用組織のデータベース中で管理されている. そのため, メーリングリストのように一つ一つ登録アドレスを更新する必要はない. また, 送信者は配送ルールの記述により柔軟に送信範囲を指定できるため, メーリングリストのようにいくつものグループを用意する必要はない. 例えば大学でのメール配信を行う場合, 研究室, 学年, 学科などのグループ毎にメーリングリストを用意しなければならない.

4.1.1 配送ルール

配送ルールとは配送範囲記述とそれに基づき送信先メールアドレスを得るクエリーを関連付けるルールである. 配送ルールは以下のように定義する.

配送ルール名
parmeter:パラメータの型
query: 送信先メールアドレスを得るための
クエリー

query 部分は SQL によって記述される. RMX は記述された配送ルール名に対応するクエリーにパラメータを挿入し, 問い合わせを行うことで送信先メールアドレスを得る. このような配送ルールを用いることにより, 利用者は簡潔な記述で配送範囲を指定することができる. 以下に配送ルール定義の例を示す.

```
grade
parameter: integer
query: select x.address from rmx x, stu-
dent s
where x.id = s.id and s.grade =" $1 " ;
```

上記の例では学年を integer 型で受け取り, それに基づいてメール配信を行う grade ルールを定義している. 図 3 のように query 部分で利用者のメールアドレスが格納されている表 rmx, 利用者に関する情報が格納されている表 student から, 学年が 3 年の学生のメールアドレスを得るクエリーを記述している.

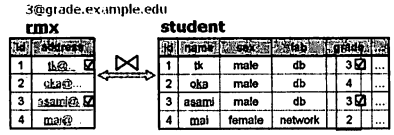

図 3 grade ルールと配送例

4.2 RMX における現行の送信制限方式

RMX ではシステムを悪用したスパムの配信を防ぐために送信を制限することができる. 現在の RMX における送信制限方式では下記の二種類の制限があり, どちらかを選択し利用者全体に適用することができる. 図 4

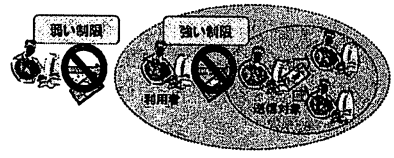

図 4 現在の RMX における送信制限

弱い制限: 送信者が RMX 利用者リストに含まれていれば送信を行える.

強い制限: 送信の際に指定した送信先範囲に送信者が含まれている場合のみ送信を行える.

弱い制限は主に外部からの RMX を利用した不要メール配信の防止を目的としている. 強い制限を用いることで RMX 利用者であっても自分が送信先に含まれないような範囲にメールを配信できなくなる. これによって不要なメールを減らすことができる.

現在のところ RMX は企業など単一の組織での利用を想定している. 後述のように, このような場合は弱い制限によって適切な運用が可能である. しかし, 複数の組織にまたがる RMX の利用や SNS のような流動性, 匿名性の高い組織での利用においては, 従来の単純な送信制限方式では問題が生じる. 本研究では配送ルールとは別に送受信許可ルールを記述することで個々の利用者に応じて柔軟に送受信許可を行う方式を提案する.

4.3 ルール記述による送信許可方式

現在のところ RMX は企業など単一の組織での利用を想定している. しかし, 複数の組織にまたがる利用, 匿名性が高いグループなどにおいて RMX を利用する場合, 運用上で次のような違いがある.

・利用者間での情報漏洩

複数の組織にまたがる利用の場合, 送信範囲の指定ミスにより誤って他の組織の利用者に情報が流れる可能性がある. 例えば大学において RMX を利用を考え

る. 3.db@gakunen.lab.example.edu のように記述し, db 研究室の 3 年生にメールを配信する場合, もし, 研究室に関する指定を忘れて 3@gakunen.example.edu のように記述してしまった場合, 大学内の全ての 3 年生に誤ってメールが配信されてしまう. このように, わずかな記述ミスにより広範囲に誤ってメールが配信されてしまう可能性がある. 従来, RMX では企業内など単一の組織での利用を想定しており, このような誤配信が起こっても情報の漏洩は企業内に留まる. しかし, 本研究で想定する複数の組織にまたがる利用でこのような誤配信が起こった場合, 共同で RMX を利用している全ての関連企業に情報が漏洩してしまう.

・利用者の把握の困難さ

特に SNS のような不特定多数が参加するグループでは企業とは違い, 利用者の把握は困難と考えられる. そのため RMX によって任意の範囲にメールを送ることができては不要メールが配信される可能性がある. このように, 複数の組織にまたがる利用の場合全ての利用者が任意の相手にメールを送信できると情報漏えい, 不要メールなどの問題がおこる可能性がある.

そこで本研究では送受信許可ルールを記述することで個々の利用者に応じて柔軟に送受信許可を行う方式を提案する. 複数の組織にまたがって RMX を利用する場合, 利用者の所属企業, プロジェクト, 役職などの個々の利用者の情報に基づいて送受信許可を行う必要がある. これらの情報に基づいて送受信の許可を行う. また, 送信先指定に利用する情報についても制限を行う必要がある. 例えば, 管理職の利用者には社員の給料, 勤続年数などを利用しての送信範囲指定を許可するが一般の利用者にはそれらを利用されたくない場合が考えられる. この場合, 管理職の利用者には RMX 中で定義された給料, 勤続年数などの配信ルールの利用を許可し, 一般の利用者にはそれらの利用を禁止する.

4.4 提案モデル

RMX におけるメール配信行為は送信者, 受信者, 送信時に利用する配送ルールで表現することができる. 本研究では配信行為, つまりこれらの組み合わせに対して許可, 不許可などを設定する. これを許可ルールと呼ぶ. さらに複数の許可ルールを組み合わせることで意図する送信許可を表現する. 許可ルールの集合を許可ポリシーとする. 利用者により配信要求がされた際には配信要求の情報と"許可ポリシーに基づき設定された許可"を照らし合わせる. これに基づき配送許可などの判断を行い, 最終的に実際の配送を行う. 図 5

4.5 送受信許可ルール

メール送受信許可ルールを Horn 節により記述する. メール送受信許可ルールは送信者, 受信者の情報

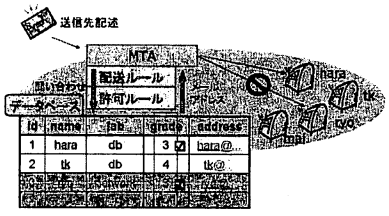

図 5 提案モデル：ルールによる送信許可

とこれらの関係とこれらに基づく送受信許可の種類, 対象となる配送ルールで構成される.

利用者によりメール配信要求がされた際に RMX システムは送受信許可ポリシーに基づいて利用者データに設定された送受信許可に従い, メール配信を行う.

4.5.1 ユーザ属性

送信者, 受信者間の関係を表すためには, まず個々の利用者に関する情報を表現する必要がある. 本研究ではこれを利用者情報と定義し, 知識ベースに記述する.

利用者属性は大きく利用者個人に関する情報と利用者間の情報に分けることができる. 前者は対象の利用者とその情報で記述され, 後者は複数の利用者とその関係で記述される. 以下にユーザー属性記述の記述例を示す.

・人物 X の役職は manager である: post(X,manager)
・人物 X の年齢は 30 才である: age(X,30)
・人物 X は企業 A に所属している: company(X,A)
・X と Y は同僚である: coworker(X,Y)
・Y は X の上司である: manager(Y,X)
・X と Y が同じプロジェクトに所属すれば, X と Y はプロジェクトメンバーである:
project_member(X,Y):- project(X,Z)project(Y,Z)

4.5.2 送受信許可ルール

送信者 S が受信者 R にメール送信許可を持つことを表す送受信許可ルールを以下の述語で記述する.

$$P(S, R, D) : -condition \quad (1)$$

P: 送信許可の種類 {allow,deny,default,log...}
S: 送信者
R: 受信者
D: 送信先指定に利用する配送ルール { 配送ルール名,all,...}
condition: オプションとして指定できる条件

送信許可 P は以下の種類から成る.
・permit: 送信を許可する
・deny: 送信を禁止する
・default: 誤送信を防止するために明示的に送信を指定した場合のみ送信が可能

・log: 該当する送信先に送信が行われる場合, メールを保存する

配送ルール D には対象となる配送ルール名もしくは全ての配送ルールが対象であることを表す all を記述する. また condition 部分で付加する条件を記述する. ここには送信者と受信者の関係などを記述する. 以下に許可ルール記述の例を示す.

・同じ企業の利用者に配送ルール company,dept による送信を許可:

```
permit(X,Y,[company,dept]):-
        company(X,Z),company(Y,Z)
```

・同じプロジェクトの利用者に配送ルール project による送信を許可:

```
permit(X,Y,[project]):-
        project(X,Z),project(Y,Z)
```

・管理職の利用者 (post='manager') にはその企業内に全ての配送ルールによる送信を許可:

```
permit(X,Y,all):- post(X, ' manager ' ),
        company(X,Z),company(Y,Z)
```

・役職がアルバイト (post='part-time') の利用者の利用を禁止する:

```
deny(X,Y,all):- post(X,'part-time')
```

4.5.3 送受信許可ポリシー

実際の企業や大学では一つの許可ルールだけでなく利用者の役職, 所属プロジェクト, 部署などに基づく様々な要求に基づいて送受信許可を行う必要がある. 以上で説明した許可ルールを組み合わせることでこのような複雑な送受信許可を表現する. この際, 複数のルールが同じ範囲に重なる場合があるため優先順位を定める. 本研究では後に記述されたルールほど優先順位が高いものとする. これによりまず広範囲に適用される一般的なルールを記述し, その上に個別の特殊なルールを記述する. 以下に送受信許可ポリシーの記述例を示す.

```
rule1: permit(X,Y,[company,dept]):-
        company(X,Z),company(Y,Z)
rule2: permit(X,Y,[project]):-
        project(X,Z),project(Y,Z)
rule3: permit(X,Y,all):-
post(X,manager), company(X,Z),company(Y,Z)
```

送受信許可ポリシーは対象となる全ての利用者に適用される. 例えば図 6 のユーザー oka, asami の場合には白抜きの範囲への送信が許可される. このように複数の許可ルール記述することで役職, 所属など利用者の情報に応じた送信許可が可能となる.

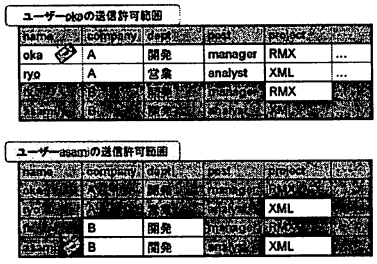

図 6 各利用者の送信可能範囲

5. まとめと今後の課題

本研究では RMX における情報漏洩, 不要メールの防止を目的としてルールを記述することで柔軟に送受信許可を行う方式を提案した. 今後はシステムの試用により有用性, 問題点を検討する. 提案手法により送信範囲を制限することで不便が生じる可能性があるが, 如何にして利便性を損なわずにセキュリティを向上させるかについて検討する. また, 本稿では条件付送信許可として default,log の二つを用意したがこれらの詳細や他の条件付送信許可について検討する.

文 献

[1] Matthew Marx, Chris Schmandt. "CLUES: dynamic personalized message filtering", Proceedings of the 1996 ACM conference on Computer supported cooperative work, Pages: 113 - 121, November 1996

[2] Mukesh Dalal. "Spam and popularity ratings for combating link spam", Proceedings of the 16th international conference on World Wide Web, Pages: 1199 - 1200, May 2007

[3] Baoning Wu, Vinay Goel, Brian D. Davison. "Topical TrustRank: using topicality to combat web spam", Proceedings of the 15th international conference on World Wide Web, Pages: 63 - 72, May 2006

[4] S/MIME and OpenPGP. http://www.imc.org/smime-pgpmime.html

[5] YASU KENJI, AKAHANE YASUHIKO, OZAKI MASAMI, SEMOTO KOJI, SASAKI RYOICHI "Evaluation of Check System for Improper Sending of Personal Information in Encrypted Mail System", Transactions of Information Processing Society of Japan Vol.46, pp. 1976-1983

[6] 高畑理, 藤沼健太郎, 石橋玲, 遠山元道. "Magic Mirror Mailing：個人情報データベースを利用する柔軟なメイル配送システム", 情報処理学会データベースシステム研究報告 Pages: 123-128 July 2001

[7] Kim Hanki, Sang-Gyu Shin, Motomichi Toyama. "A Rule-Based Mailing System for an Organization", International Workshop on INformation Processing over Evolving Networks ,June 2006