Vol.2013-DPS-154 No.50
Vol.2013-CSEC-60 No.50
2013/3/15

実運用を考慮した電子メール誤送信対策

堀田知宏[†1]　橋本正樹[†1]　辻秀典[†1]　田中英彦[†1]

企業・教育機関等組織からの情報漏えいに対する注目度が高まっている．情報漏洩の原因としては，メール誤送信によるものが高い割合を占めており，組織は誤送信対策ソフトウェア等で対策を導入している．しかし，ソフトウェアを運用する負荷の増加，それに伴う対策の形骸化，グループごとに異なる「機密情報」の考え方への対応等，誤送信対策の精度を向上させるうえでの問題が山積している．
本稿では，近年の主要なメール誤送信対策ソフトウェアにて実装されている，特定の機密情報を含むメールを外部へ送信不可とする機能に着目し，機密情報となりうる用語を運用者に自動的に提示する手法を提案する．さらに，機密情報となりうる用語は，組織全体のみでなく，部署やプロジェクトといった単位でも提示することで，細かなグループごとの機密情報送信制限に対応する．本提案により，運用負荷の軽減，機密情報の製品への登録失念等による誤送信発生リスクの低減を図る．

The measure against E-mail mistransmission in consideration of actual operation

TOMOHIRO HOTTA[†1]　MASAKI HASHIMOTO[†1]
HIDENORI TSUJI[†1]　HIDEHIKO TANAKA[†1]

The degree of attention to the information leak from organizations, such as companies and educational facilities, is increasing. E-mail mistransmission accounts for a high rate as a cause of a leak of information. The organization is coping with it by introducing mistransmission measure software etc. However, the problem for raising the accuracy of the measure against mistransmission accumulates. For example, the increase in the load which employs software, emasculation of the measure accompanying it,correspondence to the view of "confidential information" different for every group and so on.
In this paper, we pay our attention to the function which cannot send the mail including specific confidential information to the exterior.This function is mounted by main e-mail mistransmission measure software in recent years. We propose the technique of showing an operator automatically the term which can serve as confidential information. Furthermore, the term which can serve as confidential information is shown not only in the whole organization but in its post and the unit of a project.By the above, we aim at mitigation of employment load, and reduction of an e-mail mistransmission risk.

1. はじめに

企業・教育機関等組織からの情報漏えいに対する注目度が高まっている．第三者へ機密情報が漏えいすると，情報漏えいによる損害賠償，社会からの信頼の失墜などを起こし，大きな損害を被ることになる．情報漏えいの原因は数多くあるが，その中でもメール誤送信によるものが高い割合を占めている．そこで，関連研究としても多くのメール誤送信対策手法が提案されており，技術的対策，運用対策等で解決することを提案している.また,組織によっては，各ベンダが販売する誤送信対策ソフトウェアを導入して，メール誤送信リスクを低減しようと対策を講じている．

しかし，上記解決策を導入したとしても，以下の問題が残る．メール誤送信対策ソフトウェア等を導入しても，機密情報の定義や利用者による確認を利用者や運用者自身が手順に従って実施しなければ対策としての効果は望めない.つまり，メール誤送信リスクを低減するためには，利用者や運用者の負担が少なからず存在し，利用・運用条件が複雑になるほど負荷は増加する．そして負荷が増加すると，利用者や運用者の本業務の稼働時間が圧迫されることになり,結果として利用者や運用者が手順を省略等してしまう．その場合，対策ソフトウェア等を導入していても，対策が形骸化してしまい,リスクの低減が望めなくなってしまう．

本稿では，近年の主要なメール誤送信対策ソフトウェアにて実装されている，特定の機密情報を含むメールを外部へ送信不可とする機能に着目して，上記問題を解決する手法を提案する．まず，機密情報となりうる用語を運用者に自動的に提示する機能を実装し，運用者や責任者が機密情報の検討・選択に要する時間を短縮する．さらに，部署やプロジェクト単位といった小・中規模単位で提案手法を導入することで，グループによって異なる「機密情報」の定義の違いにも対応する．本提案により，運用負荷の軽減，機密情報の登録失念等によるメール誤送信発生リスクの低減を図る．

本稿の構成を示す．第 2 章では，情報漏えいおよびメール誤送信に関する研究背景を述べるとともに，関連研究，製品等で提案，実施されている対策を示し，なお残る未解決の問題をまとめ，それらの問題を受けて，本研究の目的を示す．第 3 章では，第 2 章で示した問題点を解決するための提案手法を示し,各種提案手法のアルゴリズムを示す．第 4 章では，第 3 章の提案内容の効果を検証するための評

†1 情報セキュリティ大学院大学　情報セキュリティ研究科
INSTITUTE of INFORMATION SECURITY

Vol.2013-DPS-154 No.50
Vol.2013-CSEC-60 No.50
2013/3/15

価結果を述べ，本手法が問題解決に寄与することを示す．第 5 章では，本研究のまとめを行う．

2. 研究背景

2.1 情報漏えい事件・事故の傾向

2005 年に個人情報保護法が施行されて以来，企業・教育機関等組織からの情報漏えいに対する注目度が高まっている．それに伴い，組織は各種対策を実施しているものの，個人情報漏えい事件･事故の発生が頻繁に報道されている．

日本ネットワークセキュリティ協会の報告書[1]によると，2011 年の個人情報漏えい事件･事故の件数は 1551 件，個人情報の漏えい人数は 628 万 4363 人にも及ぶ．また，個人情報の漏えいについては公表が義務付けられているが，他組織の情報，情報システムの設計情報等，その他重要情報については，公表が義務付けられていない．そのため，非公表の事件・事故も含めると，発生件数はさらに増加する可能性がある．

また，日本情報経済社会推進協会の資料[2]によると，個人情報関連事故の原因としては，いずれの年度も，紛失がもっとも多く，つづいてメールの誤送信，宛名間違い等による情報の誤送付が多いという結果となっている．本稿では，その中でも技術的対策による効果が高いと考えられるメールの誤送信に着目して，その対策方法を提案する．

2.2 メール誤送信

日本ネットワークセキュリティ協会の報告書[3]によると，メール誤送信の中でも，「誤った宛先へ送信したことがある」ケースが，全体の 80% を占めていることがわかる．つまり，誤った宛先への送信により，機密情報も第三者へ漏えいしてしまうパターンが多いことが想定される．また，「機密情報などを誤って記入したり，添付したりして送信したことがある」というケースが 11% を占めている．このケースは，宛先を誤っていない直接的な情報漏えいを経験したことを意味しており，先の「誤った宛先へ送信したことがある」と合わせると，結果として第三者への情報漏えいにつながるケースが多いことが読み取れる．

2.3 関連研究・製品

2.3.1 関連研究

1. 学習型のテキスト分類器によるメール内容分析

Graham[4]は，ベイジアンフィルタを用いて，スパムメールかどうかを判定するアルゴリズムを提案した．具体的には，メール中の単語ごとにスパムであるかどうかの確率（以下，スパム確率と称する）を求めて，計算の結果重要と判定された 15 単語を用いて，全体のスパム確率を計算するというものである．また Gray[5]は，Graham の手法を改良したものを提案した．出現回数が少ない単語のスパム確率が極端に上昇しないよう，計算アルゴリズムを改良して，誤検知の確率を減少した．

2. メール誤送信の防止・検知

1 で示したアルゴリズムを利用する等して，メール内容および宛先情報等から，メール誤送信を防止および検知する手法が数多く提案されている．

柴田ら[6][7]は，機密情報であるか否かを自動的に判別するために，電子メールの本文情報を基に，学習型のテキスト分類器を適用することで，組織にとって外部への送信が許されない機密メールと外部送信が許される非機密メールを分類可能であることを示した．辻野ら[8]は，メールの送受信者間の人間関係を利用することでメールの誤送信を防止するシステムを提案した．本田ら[9]は，組織内の利用者から送信されるメールの状態をパラメータ化し，ベイズ分類器による機械学習を利用することで，「正常な送信であるメール」を定義し，それと異なるパラメータを持って送信されたメールを誤送信と判定するフィルタリング手法を提案した．

3. 利用者への注意喚起

向井ら[10]は，メール誤送信が疑われるケースが発生したとき，インタフェースにてあえて利用者に不快感を与えることで，誤送信の可能性が高いことに気付かせ，自発的なリスク回避を支援するシステムを提案した．具体的には，過去のメール送信履歴，送信回数，登録済みのメールアドレスドメインリストを利用して，これから送信しようとしている宛先が頻繁に送信するメールアドレスであるかどうかを判断し，宛先誤りがある場合には，利用者に不快なインタフェースを提示するというものである．

2.3.2 関連製品

メール誤送信対策を実装した主要製品の調査の結果，ほぼ同様のプロセスでメール誤送信対策を実現していると考えられる．主要製品によるメール誤送信防止のプロセスの全体像を図 1 に示す．

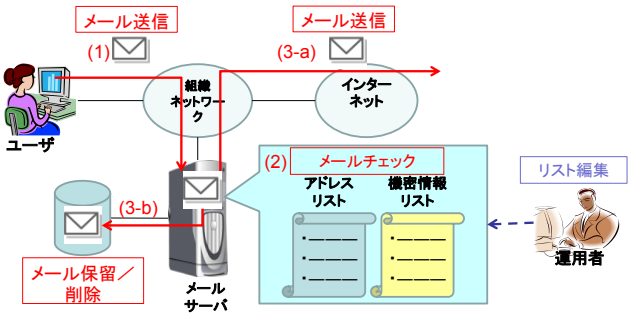

図 1 主要製品によるメール誤送信対策

Figure1 The measure against E-mail mistransmission by main products

Vol.2013-DPS-154 No.50
Vol.2013-CSEC-60 No.50
2013/3/15

図 1 中のプロセス(1)～(3)の詳細は，以下のとおりである．

1. 利用者がメールを送信する．
2. 製品に登録済のアドレスリストおよび機密情報リスト等を利用して，送信が許可されているメールであるか判定する．
3. (a)送信が許可されているメールであると判定された場合，宛先メールアドレスへメールが送信される．
   (b)送信が許可されていないメールであると判定された場合，送信を行わずにメールサーバへ一時的に保存して送信を保留する，もしくは削除する．送信を保留したメールは，上司等が送信を承認することより，宛先メールアドレスへ再送信可能となる場合もある．

2.4 現状の問題点

2.4.1 機密情報リストの運用負荷

メール誤送信対策ソフトウェアの機能を効果的に活用するためには，前述の機密情報リストの運用を滞りなく効率よく行うことが必要不可欠である．ここで運用者は，機密情報が組織の外部へ漏えいすることがないよう，機密情報リストを適宜編集する必要があるが，本作業は手動で行わなければならない．また，特定の情報が機密であるかを判断するには，あまりに日々のメール送信数が多く，情報を全て確認することは困難である．

以上の理由から，運用者の運用負荷増加により，機密情報リストへの機密情報登録忘れ，本来登録すべき情報の見逃しが発生し，情報漏えいのリスクが高まってしまう．

2.4.2 利用者によるメール誤送信確認の負荷

いくつかの関連研究や製品では，利用者に誤送信有無を確認させる仕組みを提供することで，メール誤送信リスクの低減を図っている．しかし，多くの送信メールに対して誤送信有無を利用者に確認させている場合，利用者は確認作業を徐々に負担に感じることで，確認を怠るようになり，やがて確認という対策作業が形骸化してしまう．その結果，実態としてリスクはほとんど変わらないかもしれない．

2.4.3 組織によって異なる機密情報

関連研究や製品では，組織外への機密情報送信は禁止できるものの，さらに細かな組織単位でも情報送信制限までは言及されていない．同じ組織内であっても，部署やプロジェクトごとに実施する業務は異なるため，メール送信禁止したい用語も部署等により異なると考えられる．同一の用語であっても，ある部署は送信禁止したいと考え，別の部署は送信禁止不要と考えるかもしれない．つまり，組織外部向けの機密情報リストだけで送信制限しようとすると，正常メールを誤送信メールと誤判別する False Positive，および誤送信メールを見落としてしまう False Negative の発生リスクが高まり，本業務に支障をきたす．

2.4.4 自動的なメール内容判断の限界

いくつかの関連研究では，自動的にメールを判定する手法が提案されているが，あくまでも情報システムによって自動的に可能なのは，誤送信のリスクの高低の判断であり，複雑なメールや初見のメールに対して，全て誤送信の有無を判定できるわけではない．誤送信の確率がわずかと判定されても，機密情報が含まれるメールが外部へ漏えいすれば，情報漏えいというインシデントが発生したことに変わりない．完全に対策を自動化するよりも，自動的に行う部分，手動で行う部分を切り分けることで，人の負荷を軽減しつつ誤送信リスクを低減することが望ましいと考える．

2.5 本研究の目的

本研究の目的は，2.4 節にて示した問題を解決し，運用者の負担軽減，およびメール誤送信による情報漏えいリスク低減に寄与することである．そのために，機密情報候補の自動提示，グループ単位での機密情報の提示という手法を提案する．本研究での誤送信防止対象は，メールの件名および本文とする．既存の問題点と本稿にて提案する手法との対応は，表 1 のとおりである．

表 1　問題点と提案手法の対応

Table1　Correspondence of problems and proposal techniques

現状の問題点	提案手法		
	機密情報候補の自動提示		グループ単位での機密情報の提示
	関連用語推奨	類語推奨	
機密情報リストの運用負荷	○	○	－
利用者によるメール誤送信確認の負荷	○	○	－
組織によって異なる機密情報	－	－	○
自動的なメール内容判断の限界	○	○	－

3. 提案手法

3.1 提案手法の全体像

本研究では，機密情報リストに機密情報として追加すべき用語を自動的に運用者へ追加候補として提示することで，運用者の運用負荷軽減を図る．さらに，組織内の部署，プロジェクトといった中小規模のグループを設定して，部署やプロジェクトによって異なる「機密情報」の定義にも対応できるようにする．また本提案は，あくまで運用者に機密情報の追加候補を提示するものであるため，最終的に機密情報リストに追加候補の用語を登録するかの判断は，運用者や責任者に委ねられる．それにより，False Positive お

よび False Negative の発生を最小限に留め，業務が滞る等の影響を小さくする．

本稿にて提案する手法の全体像を図 2 に示す．提案する手法は，図 1 で示した主要製品によるメール誤送信防止プロセスを補助するものであり，図 2 中の(a)～(g) が本提案手法独自のものである．図 2 に登場する用語については，表 2 にて説明する．

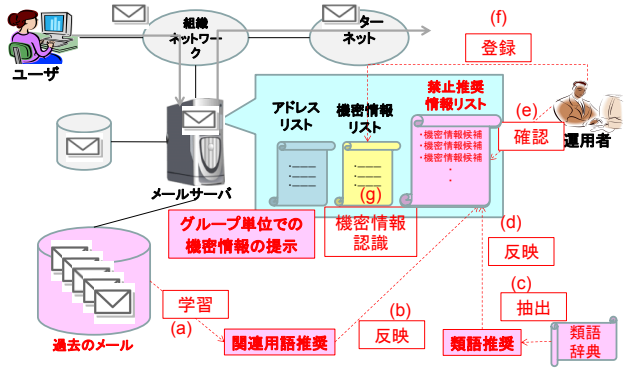

図 2　提案手法の全体像

Figure 2　The whole image of the proposal techniques

表 2　図中用語の説明

Table2　Explanation of a term in the image

用語	説明
アドレスグループ	メール送受信を制限したいグループ（部署，プロジェクト，組織等）単位ごとに設定したアドレスの集合．
機密情報リスト	外部への送信を禁止する用語一覧を記載したリスト．機密情報リストに登録された用語を含むメールは，送信禁止対象となりうる．
禁止推奨情報リスト	本研究の提案独自のものであり，機密情報リストに追加すべき用語として推奨されたものを一覧化したリスト．送信メール内に，禁止推奨情報リストに登録された用語が含まれていても，機密情報リストに未登録であれば，送信禁止対象とはならない．

提案手法のプロセス詳細は，以下(a)～(h)のとおりである．以下のうち(a)～(g)は，図 2 中の(a)～(g)の詳細を説明するものでもある．

(a)　本提案システムは，機密情報として登録すべき用語がないかを調べるために，過去のメールを解析する．

(b)　本提案システムは，メール解析の結果，機密情報として登録すべきと判定された用語について，禁止推奨情報リストへ反映する．

(c)　本提案システムは，類語辞典より，機密情報リスト中の用語の類語を抽出する．

(d)　本提案システムは，抽出した類語を禁止推奨情報リストへ登録する．

(e)　運用者は，禁止推奨情報リスト中の用語，すなわち機密情報候補として提示された用語を確認する．

(f)　運用者は，禁止推奨情報リスト中の用語のうち，機密情報と判断できる用語を機密情報リストへ登録する．

(g)　本提案システムは，運用者が(f)で登録した用語を新規に機密情報として取り扱い，新しく関連用語や類語推奨を行うためのインプット情報とする．

(h)　(a)～(g) を繰り返す．

3.2　提案手法の詳細

3.2.1 関連用語推奨機能

本機能では，機密情報リストに登録されている用語と同じメールに含まれている用語を機密情報の候補として提示する．たとえば図 3 のように，機密情報リストに「機密」という用語が登録されているときに，「決算情報をお送りします．これは機密ですので，公開不可です．」と本文に記載されたメールが送信されたとする．このとき，同メール中の用語，「決算情報」「公開不可」という用語も，外部への送信を禁止すべきメールに含まれるかもしれないと考え，機密情報となりうる候補とする．

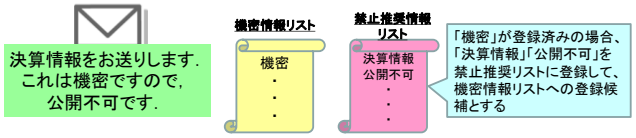

図 3　関連用語推奨機能の例

Figure3 The example of a related term recommendation function

関連用語推奨機能のアルゴリズム詳細を以下に述べる．

1. 機密情報が含まれる送信メール（以降，機密メールと称す）を形態素解析して名詞を抜き出す．抜き出した名詞は，ベイジアンネットワークのノードとする．
2. 機密情報が含まれていないメール（以降，非機密メールと称する）中の用語のうち，一定値以上全非機密メール中に存在する用語は，ノードから削除する．また，人名用語は頻出するため機密とは考えにくいケースが多いことから，ノードから削除可能とする．
3. 機密情報リスト中の機密情報から，機密情報と同じメールに含まれる用語に対して，一定数だけエッジを作成する．エッジを作成する用語は，全機密メール中に含まれる数が多いものから順に選択する．
4. ベイジアンネットワークにて，各ノード（用語）の重みを計算する．ここで，ノードのパラメータは，YES／NO の 2 種類であり，用語の重みは YES の値とする．YES はノードの用語がメールに含まれる確率，NO はノードの用語がメールに含まれない確率である．
5. 4 にて計算した用語の重み（YES の値）が一定値を超えた用語を禁止推奨情報リストへ登録する．ここで，推奨用語が機密情報と重複することを避けるため，機密情報リスト中にある用語は，禁止推奨情報リストに

は登場しないよう自動的にチェックを行う．

6. 機密情報リストの用語の重みを更新する．また，運用中に用語の重みが一定値以下になった用語は，機密情報リストからの削除候補であることを運用者に示す．

本機能を実現するにあたり，運用者が設定すべきパラメータは表 3 のとおりである．

表 3　運用者が設定するパラメータ（関連用語推奨機能）
Table3　The parameters which operators set (related term recommendation function)

パラメータを利用する手順	パラメータ
2	除外する非機密用語の閾値
2	人名用語のノードの追加是非
3	1 つの機密情報用語から作成する最大エッジ数
5	禁止推奨用語として推奨する用語の閾値
6	削除候補とする用語の閾値

3.2.2 類語推奨機能

本機能では，機密情報リスト中の用語の類語を提示して，表記揺れ等により見逃してしまう用語の機密情報リストへの登録を運用者へ促し，情報漏えいのリスクを低減する．類語の出所としては，Weblio 類語辞典[11]を用いる．また，必要以上の類語提示を避けるため，提示する類語は，Google AdWords キーワードツール[12]にてグローバル月間検索ボリュームの多い用語のみとする．

たとえば図 4 のように，機密情報リストに「機密」が登録されている場合，「機密」の類語である「秘密」「重要事項」等を候補として提示する．

本機能のアルゴリズム詳細を以下に述べる．

1. 機密情報リストから，機密情報である用語を抽出して，その類語を検索する．
2. 運用者が設定数だけ類語を抽出する．抽出する類語は，Google AdWords キーワードツールのグローバル月間検索ボリュームが高いものを優先する．
3. 抽出した類語を禁止推奨情報リストへ登録する．類語の重みは，類語元の用語の重みと原則同様だが，禁止推奨用語として推奨する用語の閾値を下限とする．

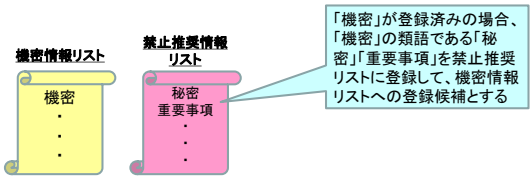

図 4　類語推奨機能の例
Figure4 The example of a class term recommendation function

本機能を実現するにあたり，運用者が設定すべきパラメータは表 4 のとおりである．

表 4　運用者が設定するパラメータ（関連用語推奨機能）
Table4　The parameters which operators set (related term recommendation function)

パラメータを利用する手順	パラメータ
2	類語推奨数

3.2.3 グループ単位での機密情報定義機能

送信制限の対象として，従来の組織（企業，教育機関等）という単位だけでなく，組織内の部署やプロジェクトといったさらに細かな単位を設定する．それらの集団単位ごとに別々の機密情報リストおよび禁止推奨情報リストを作成することで，部署やプロジェクト単位で機密情報を定義して送信制限する．本研究では，制限単位の増大に伴う運用負荷増加を防止するため，送信制限の対象とするのは，部署外，グループ外，組織外の 3 種類とする．「組織」「グループ」「部署」の用語定義は，表 5 のとおりである．

表 5　送信制限対象の用語定義
Table5　The term definition for a transmission limit

用語	説明
組織	送信制限を行う最大の単位．企業や教育機関（大学）等を指す．
グループ	複数の部署で構成された単位．複数部署が参画するプロジェクト（開発部と営業部等）等を指す．
部署	送信制限を行う最小単位．総務部，人事部，営業部等を指す．

本機能の具体的なイメージについて，図 5 を用いて説明する．たとえば部署 A から送信するメールの制限を考える．部署 A について作成する機密情報リストおよび禁止推奨情報リストは，「部署 A から，部署 A 外への送信を制限するリスト」「部署 A から，部署 A が含まれるグループ外への送信を制限するリスト」「部署 A から，組織外への送信を制限するリスト」の 3 種類である．

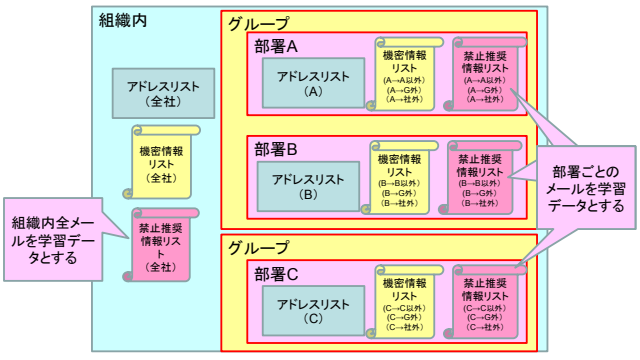

図 5　グループ単位での機密情報定義のイメージ
Figure5　The image of an confidential information definition in a group unit

3.2.4 送信メール評価

送信メールを評価し，送信制限すべきメールであるか判

定するアルゴリズムを以下に述べる．

1. 評価対象である送信メールの送信元，送信先から，適用する機密情報リストを決定する．
2. 送信メール中に機密情報リストの用語が含まれているかチェックする．
3. 送信メール中の全機密情報の重みの平均値が一定値を超えたら送信制限する．もしくは，機密情報が送信メール中に 1 つでも存在したら送信制限する．送信制限方法は，運用者が決定する．

本機能を実現するにあたり，運用者が設定すべきパラメータは表 6 のとおりである．

表 6　運用者が設定するパラメータ（メール評価）

Table6 The parameters which operators set (E-mail evaluation)

パラメータを利用する手順	パラメータ
3	送信メールの制限方法

3.3 提案手法導入における運用

3.3.1 人と役割

本提案にて設置する人物は，図 6 のとおりである．

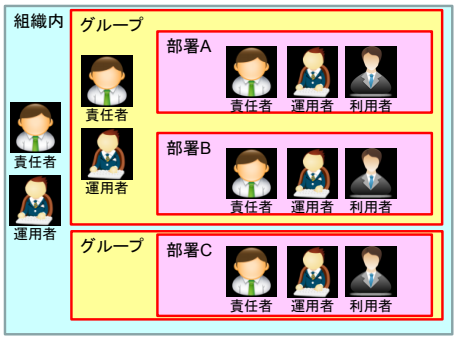

図 6　設置する人物

Figure6　The person installed

組織全体，および部署やグループごとに責任者，運用者を設置する．アドレスリストや機密情報リストの編集等の実作業は運用者が行い，設定変更の承認は責任者が行うという運用を想定する．利用者はメールを送受信する人物である．ただし，運用稼働を考慮して，部署，グループ，組織の規模次第では，業務効率を考慮して，責任者や運用者を兼務してもよい．

責任者，運用者および利用者間で意識違い等が生じないよう，各役割は表 7 および図 7 のルールに従うものとする．責任者，運用者および利用者の詳細な役割，および人の間で発生するやり取りについて，表 7 および図 7 に示す．

表 7　人の役割

Table7　People's role

人の役割	説明
責任者	・特定の用語が機密情報に該当するか否かを判断する． ・運用者からの機密情報リスト変更申請を承認／却下する． ・運用者へ機密情報登録等を依頼する．
運用者	・アドレスリストや機密情報リストの編集，禁止推奨情報リストの確認等の実作業を行う． ・利用者や責任者からの機密情報追加，変更等要求を受け付ける． ・機密情報編集について，責任者から承認を取得するため申請する． ・悪意を持った利用者が故意に機密情報を回避したメールにより情報漏えいをしないよう，利用者へ機密情報リスト中の用語を伝えることはしない．
利用者	・メール送受信を行う． ・機密情報としたい，もしくは機密情報であると認識した用語が発生したら，その旨を運用者へ伝える．

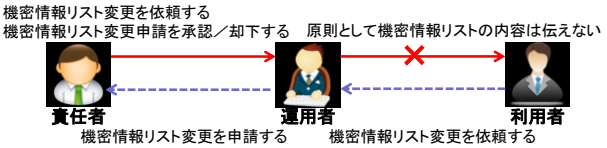

図 7　人の間で発生するやり取り

Figure7　The exchange between people

3.3.2 機密情報リストを作成するまでの運用

過去のメールから機密情報リストを作成するまでの運用プロセスを以下に示す．

1. 機密情報を検討して，機密情報リストを作成する．
2. 過去の送信メールを収集する．
3. 表 3，表 4，表 6 にて示したパラメータを指定する．
4. 3.2.1 節から 3.2.3 節の各アルゴリズムを動作させる．
5. 禁止推奨情報リストを参照する．
6. 禁止推奨情報リストから機密情報とする用語を選択して，機密情報リストへ登録する．

3.3.3 機密情報リスト作成後の運用

運用者が運用中に留意すべき点を以下に示す．

- 運用中，必要に応じて各種パラメータを変更して，組織の状況に合わせた設定により送信制限する．
- 登録済みの機密情報を早急に例外扱いしたいときは，例外設定をする．
- 機密情報リストおよび禁止推奨情報リスト上で，削除候補として表示された用語があったときは，必要に応じてリストから削除する．

4. 評価

4.1 評価観点

本提案を評価するにあたっての観点は以下である．

- 適切な用語が禁止推奨情報リストに登録されるか．
- 過去のメール等から機密情報リスト，禁止推奨情報リ

ストを作成後，送信メールが適切に送信制限されるか．

4.2 評価環境

本提案の評価環境は表 8 のとおりである．

表 8　評価環境

Table8 Evaluation environment

項目	値	備考
機密情報リストに登録済の用語	A-ORIGINAL-FRAMEWORK 厳秘	“A-ORIGINALFRAMEWORK”とは，部署 A 独自のセキュリティリスク分析フレームワークであり，社内にもまだ非公開であるため，部署 A 以外には機密扱いの情報である．
学習メール数	130 通	ある 1 週間のうちに業務にて送受信したメールを模したものを利用．
機密メール数	30 通	本表の「機密情報リストに登録済の用語」が含まれるメールを指す．

運用者が設定するパラメータは，表 9 のとおりとする．

表 9　運用者が設定するパラメータ

Table9　The parameters which operators set

パラメータ	値
除外する非機密用語の閾値	0.6
人名用語のノードの追加是非	追加しない
1 つの機密情報用語から作成する最大エッジ数	10
禁止推奨用語として推奨する用語の閾値	0.3
削除候補とする用語の閾値	0.299
類語推奨数	2
送信メールの制限方法	全機密情報の重みの平均値

4.3 学習メール

本評価で用いる学習メールの例を示す．図 8 は機密メールの例，図 9 は非機密メールの例である．

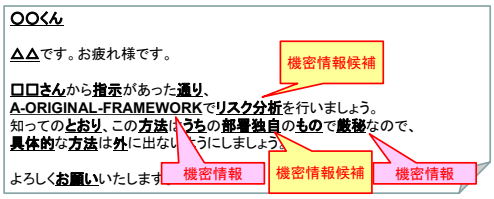

図 8　機密メールの例

Figure8　The example of confidential mail

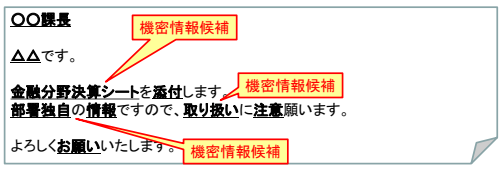

図 9　非機密メールの例

Figure9　The example of non-confidential mail

図 8 には，表 8 の機密用語が含まれており，その他機密情報候補としても，“リスク分析”“部署独自”がある．図 9 は，本提案適用前は非機密メール扱いだが，“部署独自”等，機密情報と推測される用語が存在する．

4.4 評価結果

4.4.1 禁止推奨情報リストの用語の評価

1.　本提案適用時の評価

本提案により禁止推奨情報リストに登録された用語，およびその重みを表 10 に示す．

表 10　評価結果

Table10 Evaluation result

推奨用語	重み
リスク分析	0.790
部署独自	0.684
取り扱い	0.468
了解	0.430
うち	0.333
秘密	0.300
極秘	0.300

“リスク分析”は，禁止推奨されるとともに，重みも比較的高い値となった．この用語は，他部署にとっては機密情報でないかもしれないが，今回の評価では，機密用語である“A-ORIGINAL-FRAMEWORK ”がリスク分析フレームワークそのものであり，“リスク分析”を機密扱いにしなければ，フレームワーク関連のメールが外部へ漏えいするかもしれない．固有名詞を機密情報として登録していればよいと運用者が考えていた場合には，新たな気付きを与えられ，リスク低減につながると考えられる．

また，“部署独自”“取り扱い”が推奨された．これらは，本提案前の段階でも，運用者がメールの内容まで詳しくレビューすれば，機密情報として登録されたかもしれない．しかし，実際には全メールを詳細にレビューするのは時間上困難であり，これらの用語を見逃す可能性がある．即ち本提案により，詳細レビューを行わずに機密情報とすべき用語を発見でき，運用負荷軽減に寄与したと考えられる．

一方で，“了解”，“うち”といった，機密情報とは言い難い汎用的な用語も推奨された．これらの用語は，学習データが豊富になるにつれ，非機密メールにも頻出すると考えられる．非機密メールでの出現頻度が高まれば，パラメータ次第で禁止推奨情報リストから除外可能であるため，学習が進むにつれて推奨されなくなると予想される．

2.　機密情報リストに用語を新規登録した場合の評価

禁止推奨情報リストの用語を機密情報として新規登録した場合について考察する．ここでは，表 10 の結果を受けて，“リスク分析”，“部署独自”，“取り扱い”を機密情報リストに新規登録した場合の結果を表 11 に示す．

表 11　評価結果（用語を新規登録した場合）

Table11 Evaluation result（When we register new terms）

推奨用語	重み
注意	0.459
了解	0.443
秘密	0.300
極秘	0.300

推奨用語	重み
処理	0.300
操作	0.300

“注意”が新たに禁止推奨情報リストに登録された．この用語は，“取り扱い”と同じメールで使うことが多い．“取り扱い”という推奨用語を新規登録することで，さらに新しい機密情報候補を発見できた．

4.4.2 送信メールの評価

送信メールについて評価したときの結果を示す．送信メール評価に用いる具体的な機密情報リストは表 12，評価するメールは図 10 とする．表 12 の機密情報リストには，4.4.1 節の結果を受けて禁止推奨された用語数個を登録している．

表 12　送信メール評価時の機密情報リスト

Table12 Evaluation result

機密情報	重み
A-ORIGINAL-FRAMEWORK	0.830
部署独自	0.798
リスク分析	0.790
取り扱い	0.481
秘密	0.300
極秘	0.300
厳秘	0.100

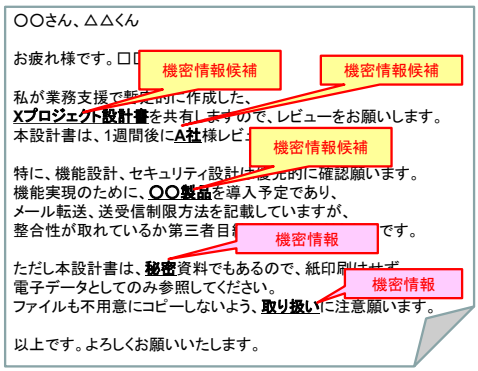

図 10　評価メール

Figure10　Evaluated mail

図 10 に含まれる機密情報は，“秘密”，“取り扱い”であり，機密情報の重みの平均値は約 0.391 である．すなわち，送信制限する閾値を 0.3 以上であれば送信制限可能である．新規プロジェクト開始直後等，機密情報の用語の登録漏れが発生しやすい時期には，送信制限する閾値の初期値を低くし，徐々に閾値を高めていく方法が有効と考えられる．

5. おわりに

本研究では，運用負荷軽減および情報漏えいリスク軽減を目的としたメール誤送信対策の提案手法を示した．具体的には，機密情報候補を自動的に提示し，機密情報検討時間を短縮できる可能性を与えた．また，小・中規模ごとに機密情報を管理することで，部署等ごとの要望に対応可能とした．さらに，運用者が設定する各種パラメータを設け，部署等個別事情を考慮して対策レベルを調整可能とした．

評価では，事前定義した機密情報以外にも，機密情報候補が提示されることを確認できた．また，事前定義した機密情報は含まれなくとも，本提案により推奨された用語を機密情報として登録すれば，機密である可能性が高いメールも送信制限できることを確認し，誤送信対策漏れにより発生するリスクを低減することに寄与した．今後は，実際の業務メールに対して本提案を適用し，推奨用語や重みの変化，適切なパラメータ等を考察する必要がある．

参考文献

[1] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ，情報セキュリティ大学院大学原田研究室・廣松研究室：2011 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，NPO 日本ネットワークセキュリティ協会，NPO 日本ネットワークセキュリティ協会（オンライン），入手先 <http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.2.pdf>（参照 2012-12-08）．

[2] 一般財団法人日本情報経済社会推進協会（JIPDEC）プライバシーマーク推進センター：平成 23 年度「個人情報の取扱いにおける事故報告にみる傾向と注意点」，プライバシーマーク制度，一般財団法人日本情報経済社会推進協会（JIPDEC）（オンライン），入手先 <http://privacymark.jp/reference/pdf/H23JikoHoukoku_120712.pdf>（参照 2012-12-08）．

[3] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ：2011 年情報セキュリティインシデントに関する調査報告書～発生確率編，NPO 日本ネットワークセキュリティ協会，NPO 日本ネットワークセキュリティ協会（オンライン），入手先 <http://www.jnsa.org/result/incident/data/2011incident_survey_probability.pdf>（参照 2012-12-30）．

[4] Paul Graham: Better Bayesian Filtering, Paul Graham(online)，入手先<http://paulgraham.com/better.html>(参照 2012-12-08).

[5] Gray Robinson: A Statistical Approach to the Spam Problem, Linux Journal, Linux Journal(online)，入手先 <http://www.linuxjournal.com/article/6467/>(参照 2012-12-08).

[6] Yerazunis, W.S., Kato, M., Kori, M., Shibata, H. and Hackenberg, K. :Keeping the Good Stuff In: Confidential Information Firewalling with the CRM114 Spam Filter & Text Classifier, White Paper for Black Hat USA 2010(2010).

[7] 柴田秀哉，加藤守，郡光則，Yerazunis, W.S.：多クラス分類によるメール誤送信検出手法，日本データベース学会 Forum 2011 B5-4（2011）．

[8] 辻野友孝，伊藤太樹，柿元宏晃，加藤健太，白松俊，大囿忠親，新谷虎松：メール履歴を利用した学習に基づく誤送信メール推定システムの試作，第 72 回情報処理学会全国大会論文集（情報処理学会），pp.2-739 - 2-740（2010）．

[9] 本田致道，佐藤直：配送情報の機械学習による迷惑メールのフィルタリング，日本セキュリティ・マネジメント学会誌，vol.26（1），pp.15-28（2012）．

[10] 向井未来，藤原康宏，村山優：メール誤送信を防止する不快なインタフェースの評価システムの実装，マルチメディア，分散，協調とモバイル（DICOMO2011）シンポジウム，pp.1490-1497（2011）．

[11] Weblio 辞書：類語辞典・シソーラス，Weblio 辞書（オンライン），入手先<http://thesaurus.weblio.jp/>（参照 2012-12-08）．

[12] Google：Google AdWords キーワードツール，Google（オンライン），入手先 <https://adwords.google.co.jp/select/KeywordToolExternal>（参照 2012-12-08）．