なりすましメール対策における自己の証明手段に関する考察と試作

伊藤 俊一郎[1,a)]　小林 和真[1]　門林 雄基[1]

概要：なりすましメールをきっかけとした情報流出等の被害が社会問題となっている．対策として S/MIME を用いた電子署名が効果的であるものの，普及率等の問題がある．本研究では，S/MIME で使用する電子署名に代わる認証要素として Canvas フィンガープリントに着目し，なりすましメール対策への活用について考察した．結果，フィンガープリントとメール本文のハッシュ値を利用することで，メールのやり取りをしたことがある送受信者間でなりすましを看破できることを示した．提案手法の実装はメーラーとしての普及率や拡張機能の開発サポートに優れている Thunderbird アドオンを利用し試作した．

キーワード：なりすましメール，Canvas フィンガープリント，認証

On The Use of Device-Intrinsic Fingerprints against Spear-Phishing E-mail Threats

Shun'ichiro Ito[1,a)]　Kazumasa Kobayashi[1]　Yuki Kadobayashi[1]

Abstract: Damage from information leakage caused by spear-phishing e-mail is a social problem. S/MIME is an effective, yet insufficient countermeasure. In this work, we focused on canvas fingerprint to substitute for S/MIME's digital signature and considered the utilization as a countermeasure against spear-phishing e-mails. As a result, we showed that senders and recipients who have exchanged e-mails can detect spear-phishing e-mails by using the fingerprint and e-mail's hash value. In order to consider both penetration rate and development support, we implemented a prototype as a Thunderbird add-on.

Keywords: Spear-phishing e-mail, Canvas fingerprint, Authentication

1. はじめに

電子メールはインターネットで利用されているアプリケーションであり，現代において重要な役割を担っている．このアプリケーションを利用したサイバー攻撃が存在し，その中でもなりすましメールは脅威が大きいサイバー攻撃の手口の 1 つである [1].

なりすましメールは，攻撃者が他人や実在する組織等を電子メールにおいて騙り，標的となるユーザに送りつけるメールである．メール受信者は巧妙に作成されたメールにより，なりすましメールと気付かずに添付ファイルの開封や本文記載の URL を押下してしまう．結果，マルウェアに感染し，攻撃者が目的とする情報窃取等を達成されてしまう．なりすましメール対策は存在するものの，なりすましメールによる被害は依然として報告されており [2]，被害を受けた組織は信用の失墜や損害対応に追われ，被害は多大なものとなる．

本研究では，なりすましメールに関する分析を行うとともに既存対策の問題について調査した．複数の既存対策は，それぞれでなりすましメールに対応できる状況が異なり，また効果的な対策の一つである S/MIME が普及していない等の問題があることが判明した．メールにおいて身元を証明する認証要素を有することでなりすましを看破で

[1] 奈良先端科学技術大学院大学
Nara Institute of Science and Technology
[a)] E-mail:ito.shunichiro.in0@is.naist.jp

表 1 既存対策の効果及び問題点

	効　果	問題点
ウイルス対策ソフトウェア	既知のマルウェアを検知・感染防止	未知のマルウェアの対応
送信ドメイン認証	送信元ドメイン詐称防止	ドメイン詐称以外の対応
電子署名	信頼できる第三者による送信元メールアドレスの保証	Web メール・スマートフォンの多くが未対応
		高コスト

きるという考えのもと，バイオメトリクス情報や電子フィンガープリント等の認証要素を調査比較し，既存対策の問題点を補う手法について考察した．考察結果を踏まえた提案手法として，Canvas フィンガープリントをメールでの認証要素として利用することにより，メールでやり取りをしたことがある送受信者間において，既存対策よりも低コストでなりすましメールに対応できることを示した．

2. 既存対策

本節ではなりすましメール対策に関する既存の商材，技術及び研究について述べる．各対策の効果及び問題点をまとめた結果を**表 1** に示す．

2.1 ウイルス対策ソフトウェア

コンピュータをマルウェアから保護するために，ウイルス対策ソフトウェアの導入が普及している．ウイルス対策ソフトウェアの主な検知方式としては，パターンマッチング，レピュテーション及びヒューリスティック技術を利用した検知手法がある．これらの技術の活用により，多くのマルウェアを検知し感染を未然に防ぐことが可能となっているが，対応できないケースもある．例えば標的型攻撃は，標的と定めた組織が使用しているウイルス対策ソフトウェアを事前に調査し，組織が使用している対策では検知されないマルウェアを使用して攻撃する場合がある．

なりすましメールにおいても同様の状況が想定され，メールの悪性添付ファイルや本文記載 URL が先述の理由により検知できない可能性がある．これまで述べた対策以外に，攻撃者が送信する実際の標的型メールが持つ特徴を分析し，その情報をもとに悪性メールの検知を行う手法を提案した研究がある [3]．また，標的型メールにおいて実際に使用されたメールアドレスの中には，Google 検索で複数ヒットするメールアドレスが存在しており，そのメールアドレスを使用したなりすましメールの危険性について言及している．この手法はなりすましメールに対しても有効であるが，巧妙化したなりすましメールに対応するには，抽出する特徴を逐次更新していく必要があり，ウイルス対策ソフトウェア同様に，未知の脅威に対応するまでの間に標的が脅威に晒される危険性がある．

2.2 送信ドメイン認証

送信ドメイン認証は受信したメールから取得した情報をもとに，メール送信者の身元を送信元ドメインに問い合わせて検証する手法である．送信ドメイン認証を用いることで，改ざんが可能な差出人のメールアドレス等の詐称に対応できる．送信ドメイン認証には主に Sender Policy Framework（SPF）と Domain Keys Identified Mail（DKIM）の 2 つがある [4]．

SPF は送信者メールアドレスのドメイン名をもとに，当該 DNS サーバに送信元メールサーバの IP アドレスを問い合わせる．送信元メールサーバの IP アドレスが問い合わせ先の DNS サーバに存在すれば，送信元メールアドレスは示された送信元メールサーバから確かに送信されたものであることが保証される．また，DKIM は送信側でメールに対して秘密鍵を使用して電子署名を作成付与して送信する．受信側では送信元の DNS サーバに公開鍵を問い合わせて電子署名を検証することで，メールの送信元ドメインが詐称されていないことを確かめる．

SPF，DKIM ともに詐称していないドメインからメールが送信された場合は，悪性メールであってもそれを看破することはできない．加えて，SPF は送信側サーバの設定ミスやメールが転送された際にはエラーとなる場合があり，DKIM ではメーリングリスト使用時に署名元のメールヘッダや本文が書き換えられないように注意する必要がある．なお，普及率としては SPF が 94.31%，DKIM が 39.84 %である [5]．

2.3 電子署名

電子署名を利用した代表的な技術として S/MIME がある．S/MIME は Public Key Infrastructure（PKI）を利用しており，公開鍵の信頼性を高めている．S/MIME を使用することで送信側でメールに電子署名を付加し，受信者側で送信者の公開鍵を使用して電子署名を検証することで，なりすましメール対策として活用できる．

現在では主要な電子メールアプリケーションの多くは S/MIME に対応しているものの，Web メール等の非対応アプリケーションが未だ多く存在することが問題である．また，携帯電話等においては電子署名付きメールを受け取らない環境が存在することや，メールアドレスと関連付けられた電子証明書を購入する必要があることが普及を妨げる要因になっているとの調査結果がある [6]．

図 1 サイバーキルチェーンモデル

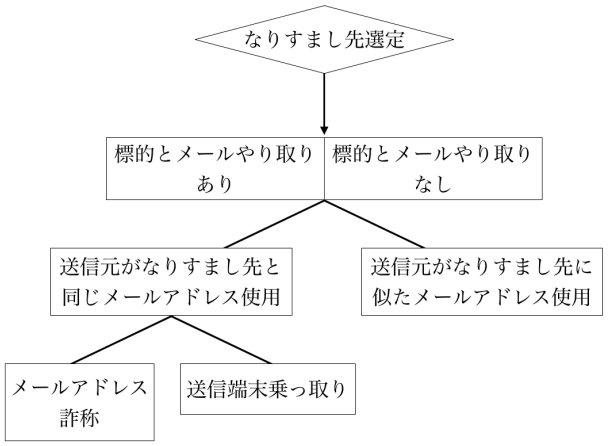

図 2 なりすましメール分類

3. なりすましメール対策における認証要素

本節ではなりすましメール及び既存対策について分析し，なりすましメールに有効な対策について検討する．

3.1 なりすましメール分析

なりすましメールによりメール受信者が感染するまでの状況について分析する．はじめに攻撃者は自らが欲しい情報を有するユーザを選定（もしくは不特定多数）し，標的となるユーザをマルウェアにより感染させるための手段を準備する．その手段としてなりすましメールが使用されることがある．なりすましメールを使用することがある標的型攻撃を例にとると，攻撃者は標的を感染させ目的を達成するまでに，**図 1** に示すようなサイバーキルチェーンモデルで定義される 7 つのフェーズを経るとされている [7]．その中でなりすましメールはマルウェアをユーザに送りつける配送段階で使用される．なりすましメールは，標的となるユーザがメールの添付ファイルを開封もしくは本文記載の URL を押下させるよう仕向けるために，標的が普段メールでやり取りしている相手や信頼出来る機関になりすましてメールを送りつける．標的となったユーザはなりすましメールが正規のメールと信じ込み，マルウェアを含んだ添付ファイルを開封等して感染してしまう．

なりすましメールにより受信者が感染するまでには，攻撃者が使用する手段によってなりすましメールを複数に分類できる．なりすましメールの分類を**図 2** に示す．なお，なりすまし先のメールアドレスを hoge@example.com と仮定し，以下で説明する．

攻撃者はなりすましメールを作成する際に，標的が油断するようななりすまし先を選定する．この時，標的がメールでやり取りをしたことがある相手か，新規送信元の相手かを選択する．標的がメールでやり取りをしたことがある相手であれば標的を油断させやすい利点がある．特に，攻撃者が送信者と受信者の間に入って両者になりすます場合は中間者攻撃と呼ばれる．この状況においては，送受信者の情報を取得するための労力が攻撃者に必要になる．一方で，新規送信元になりすます場合は警戒される可能性が高いが，標的に関する調査のコストが低く，件名や本文の工夫によって油断させられるといった利点がある．

次のステップとして，送信元メールアドレスをなりすまし先に似せる場合と，同じ場合の 2 通りが考えられる．なりすまし先に似せたメールアドレスの場合，hoge1@example.com のようにドメインを詐称していれば送信ドメイン認証技術により看破できる．しかし，もしも hoge@example.net のようになりすまし先に似ているが別のドメインから送信されたなりすましメールには対応できない．そのため，S/MIME を使用した電子署名やメールからの特徴抽出等による悪性判別により判断するしかない．送信元がなりすまし先と同じメールアドレスを使用する場合では，更に 2 通りの状況が考えられる．1 つは，同じメールアドレスを使用し詐称する場合である．この場合は，送信ドメイン認証や電子署名により判別が可能となる．2 つ目の状況としては，ユーザがメールを送信するアプリケーションを含むデバイスを乗っ取られた場合である．この場合は，送信ドメイン認証や電子署名も対策としての効果は発揮できないので，送られてくるメールの添付ファイルや本文から悪性メールか否かを判断するしか方法はない．

3.2 自己証明のための認証要素

なりすましメールの分類により，既存対策で対応できる状況が異なることが分かった．特に S/MIME による電子署名は，信頼出来る第三者から発行された電子証明書により送信者の身元を検証するため，なりすましメールには効果的である．しかし，2 節で述べたように S/MIME を使用した電子署名は，電子証明書取得コスト等の理由により，まだ十分には普及していない点が問題である．そこで本研究では，S/MIME を使用した電子署名とは別に，身元を証明する他の認証要素について調査し，なりすましメール対策としての有効性を考察する．

表 2 認証要素比較

	SYK	SYH		SYA	SYK+SYH	SYH+SYA
手法 (例)	パスワード	OTP	電子フィンガープリント	顔認識	U2F	UAF
利　点	広く浸透	推測困難	推測困難	記憶携行必要なし	高い機密性	高い機密性
	低コスト	記憶必要なし	記憶必要なし	模倣困難		記憶必要なし
		認証器必要なし	認証器必要なし			認証労力小
			認証労力小			プライバシー対策
欠　点	忘却の可能性	認証労力大	不定期に値変化	認証精度	忘却の可能性	高コスト
	認証/管理労力大	高コスト (一部)		漏洩時変更困難	認証労力大	認証器携行
	複数の脆弱性	トークン携行 (一部)			高コスト	
					認証器携行	

認証はインターネットにおいて重要な要素である．インターネットの特性上，通信の相手先が直接見えない場合が多い．そのため様々な認証方式が策定されており，主に以下の認証要素を利用してインターネット上で認証を行う．

(1) Something You Know（SYK）
　ユーザが知り得る情報．例: パスワード
(2) Something You Have（SYH）
　ユーザが所持しているもの．例: トークン
(3) Something You Are（SYA）
　ユーザの特徴．例: 指紋

電子メールでの認証としては，Web メールのユーザログインや，メールごとに電子署名等の認証要素を付加する方式が存在する．本研究においては，メールごとに認証要素を付加する方式を対象とする．メールごとに認証要素を付すことで，正規のメールとなりすましメールの区別が期待できる．以上を踏まえ，認証要素を電子メールにおける自己証明手段とした場合について，3 種類の認証要素に基づき調査した結果を**表 2** 及び以下に示す．

3.2.1 Something You Know

ユーザが知り得る情報を使用して認証するのが SYK である．SYK の代表的な認証要素としてはパスワードがある．パスワードは広範多岐にわたる場面で使用され，多くのユーザが慣れ親しんでいる認証要素でもある．パスワードは特別な認証器を必要とせずに，記憶情報のみで認証できるため，認証に必要なコストは低い．一方で，記憶情報のためパスワードを忘却する危険性や，複数のパスワードを管理しなければならないという欠点もある．また，パスワードには複数の脆弱性が存在することが広く認識されている．ユーザがパスワード設定を行う場面では，パスワードに設定する文字数が短い，辞書にある文言を使用することで推測が容易である等の脆弱性がある．これらのパスワードを使用した場合には，ブルートフォースアタックや辞書攻撃等のパスワードクラッキングツール [8] により，攻撃者にパスワードが漏洩してしまう可能性がある．また，パスワードの管理に関する暗号及び認証アルゴリズムの脆弱性を突かれ，パスワードが解読もしくは窃取される可能性も存在する．

Web におけるユーザ認証の場合は，一度パスワード等を入力し認証されることで，ログアウトもしくは一定時間経過しない限り再入力の必要はないが，メールにおいては当てはまらない．ユーザによっては 1 日に多くのメールを送信することがあるが，メール送信の都度にパスワード等を入力するのは，ユーザにとって認証にかかる労力が大きい．

3.2.2 Something You Have

SYH として，ワンタイムパスワード（OTP）や電子フィンガープリントがある．OTP は一度限りしか使用されないパスワードであり，一定時間ごとに変更される．OTP は主に 2 段階認証で使用されており，ユーザ名とパスワードを入力した後に取得した OTP を入力することで，ユーザ認証時のセキュリティを強化している [9]．OTP の取得方法はハードウェア/ソフトウェアトークン [10] を利用する方法と，SMS やメールで取得するトークンレスがある．電子フィンガープリントは特定の要素からハッシュ値を生成し，そのハッシュ値を比較することで電子的な同一性を確認する．電子証明書の識別，Web 上でのユーザトラッキング等に使用される．また，SYH と SYK を組み合わせた認証方式として Fast IDentity Online Alliance（FIDO）が提唱する Universal 2nd Factor（U2F）がある [11]．U2F は Web 認証においてユーザが SYK による認証を行った後に，U2F プロトコルに対応した U2F デバイスを使用して認証を行う．U2F プロトコルは Web サービスを提供する企業等のサーバに U2F デバイスの所持情報を事前に登録し，認証時にユーザ名とパスワードを入力した後に，ラップトップ等に接続した U2F デバイスのボタンを押下する等のアクションを示すことでユーザ認証が行われる．

SYH をメールでの認証に利用する状況を考えると，OTP は認証器を必要としない，パスワードの脆弱性を補える，記憶する必要がないという利点はあるが，パスワード同様にメール送信の都度に入力する手間がかかり，加えて OTP 自身を取得するという手間も増える．また，OTP の取得方法によってはトークンを取得し携行する必要がある．電子フィンガープリントは既に手元に存在する情報を数値化

するため記憶の必要がなく，数値を比較することで検証するので，認証器を使用せずにユーザにとって透過的な認証が行える．そして，電子フィンガープリントを作成するための要素によっては，フィンガープリントが頻繁に変化することが予想される．攻撃者にとって値が推測しづらいという反面，電子メールでの認証要素として考えた場合にはフィンガープリントの変化を送受信者で逐次共有する必要がある．理由として，普段メールでやり取りしている相手のフィンガープリントが新しい値に変化した際には，メール受信者にとって新しいフィンガープリントは新規送信者とみなされてしまうためである．U2F は SYK と SYH の組み合わせのため，比較的機密性が高い．そして，パスワード等の入力が必要であるものの，SYK に加えアクションを起こすのみで認証を行えるので，OTP に比べ認証時の労力は少ない．しかし，U2F デバイスを取得し携行しなければならないというコストと手間がかかる．SYK の要素も含んでいるため，パスワード同様に忘却の危険もある．

3.2.3 Something You Are

SYA は主にバイオメトリクス情報を使用する．SYA を使用した認証の例として，指紋認証 [12]，顔認識 [13]，キーストローク認証 [14]，タッチスクリーン認証 [15] 等がある．SYA は主に 2 種類に分類され，身体的特徴と行動的特徴がある．身体的特徴は指紋や虹彩等の特定の個人しか持ち得ない身体的情報であり，顔認識等が該当する．また，行動的特徴は個人が持つ行動の癖を読み取ることでユーザ認識を行う．例としてキーストローク認証がある．近年ではスマートフォンにおける指紋認証や銀行における指静脈認証 [16] 等，SYA の活用が普及してきている．

また, SYA と SYH を組み合わせた認証方式として, FIDO が提唱する Universal Authentication Framework（UAF）[17] がある．UAF に対応するデバイス上にてバイオメトリクス情報等を使用してユーザ認証を行う．そのため，U2F よりもデバイス紛失時におけるセキュリティ性が高いというメリットがある．UAF はプライバシー漏洩のリスクが考慮されており，バイオメトリクス情報を認証先に直接送付するのではなく，手元の UAF デバイスにおいて検証され，その検証結果が認証先に送付される．よって，ユーザ認証過程においてユーザのバイオメトリクス情報が漏洩することはない．しかし，認証器を取得するコストが発生し，認証時には携行していなければならない．

バイオメトリクス情報は認証要素が模倣困難であり，認証要素自体がユーザに備わっているため記憶する必要がないという利点があるが，プライバシーに関する問題や認証精度に関わる安全性と利便性のトレードオフ関係が課題としてある．特に，多数の宛先に情報を送信するメールにおいてバイオメトリクス情報を認証要素として使用する場合には，UAF のようなプロトコルや秘密分散 [13] によるプライバシー漏洩対策が必須である．また，認証要素が漏洩した場合には，その一意性から認証要素の変更が困難である．

4. Canvas フィンガープリントによるなりすましメール対策

3 節において様々な認証要素をメールにおける自己証明手段とした場合について考察した．本研究では，特別な認証器を必要とせず，かつユーザにとって認証労力が小さい電子フィンガープリントに着目する．

電子フィンガープリントには複数の種類が存在し，様々な場面で使用されている．その中でも Web 上でのユーザトラッキングに使用され，JavaScript が動作する環境であればフィンガープリントを取得できるという認証要素取得の容易さから，Canvas フィンガープリントを利用したユーザ識別 [18] に着目した．本節では，なりすましメール対策における自己の証明手段としての Canvas フィンガープリントの活用法について示す．なお，提案手法の実装にあたってはメーラーとしての普及率が高く，かつ拡張機能の開発サポートに優れている Thunderbird において，アドオンを利用し試作した．

4.1 Canvas フィンガープリント

Canvas は HTML5 の要素であり，ブラウザ上でプログラマティックに図を描画する機能を提供する．Canvas フィンガープリントは，Canvas を利用して描画したフォント等を暗号学的ハッシュ関数を利用して変換することでフィンガープリントとなるハッシュ値を得る．文献 [18] の研究では，Canvas によるフィンガープリントは OS，ブラウザ，GPU 等の影響を受け，その値を用いることでユーザを一意に識別できる可能性を示している．

メールにおいてユーザ識別を行う際に，Canvas フィンガープリントが不定期に変化することによる誤認識が予想される．そのため，フィンガープリントの変化要因を調査する必要がある．変化要因について調査した結果を**表 3** に示す．本調査では，OS とブラウザの組み合わせによる変化要因について調査した．OS 及びブラウザともに，ソフトウェアバージョンアップによりフィンガープリントが変化することが判明した．また，ブラウザの同バージョン内での修正に伴うアップデートにおいては，基本的にはフィンガープリントは変化しないが，一部では値変化が確認された．以上より，ブラウザのバージョンアップに伴い，多くの場合でフィンガープリントが変化することが分かった．Thunderbird で提案手法を実装した場合においても，Thunderbird のバージョンアップに伴いフィンガープリントが変化すると予想できる．なお，スマートフォン OS Android のブラウザ（Chrome，Firefox）においても Canvas フィンガープリントを取得できることを確認した．よって，スマートフォンを使用した電子メールにおいても提案手法を用いたユーザ認証は可能であると推察する．

表 3　Canvas フィンガープリント変化要因

OS	ブラウザ フィンガープリント	
Ubuntu 16.04 LTS	Firefox 46.0 2267853321	Firefox46.0.1 2267853321
	Firefox 47.0 1083076567	Firefox 47.0.1 2402789525
Ubuntu 15.10	Firefox 47.0 3701472313	Firefox 47.0.1 3701472313
Ubuntu 14.04 LTS	Firefox 47.0 3277308921	Firefox 47.0.1 3277308921
OS X 10.10.5	Safari 9.1.1 1942892720	Safari 9.1.2 161806425

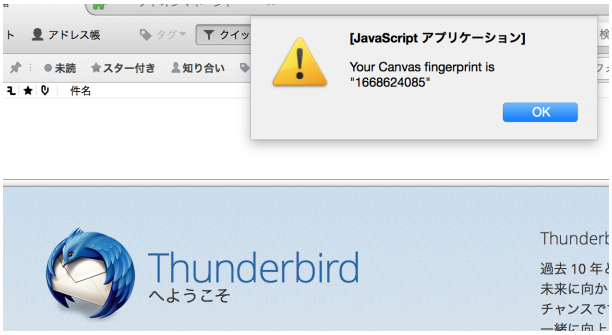

図 3　Thunderbird アドオンによる Canvas フィンガープリントの取得

次に，Thunderbird にて Canvas フィンガープリントが利用可能か調査を行った．Mozilla が開発提供を行っている Web ブラウザの Firefox やメーラーの Thunderbird においては，アプリケーションに新たな機能を追加できるアドオンを開発実装することが可能である [19]．Canvas フィンガープリントをメールにおいて認証要素とする場合には，生成されるフィンガープリントをメーラーにおいて取得できることを確認する必要がある．そこで Thunderbird にてフィンガープリントを取得するアドオンの開発を行った．結果，**図 3** に示すように Thunderbird にて Canvas フィンガープリントを取得できることを確認した．

4.2　提案手法利用想定

Web 等においてユーザ認証を行うための過程として 2 つのフェーズが必要である．1 つ目のフェーズは，ユーザの身元を証明する要素を認証システムに登録するフェーズである．そして 2 つ目のフェーズとして，登録した認証要素によりユーザの身元を検証するフェーズがある．本項では，それぞれのフェーズにおいて提案手法を効果的に使用するために必要な手順について示す．提案手法を利用するための想定環境は以下のとおりとする．なお，想定環境の設定にあたり本研究では，なりすましメールに対する効果を確認するため，メール配送時等における攻撃者による認証妨害は起こらないものと仮定する．

- 電子メールのやり取りを過去にしたことがある 2 人の正規ユーザが存在（Alice，Bob）
- 攻撃者が Bob の持つ情報を窃取するために Alice になりすまし，なりすましメールを Bob に送付
- 攻撃者は Alice のメールアドレスを詐称
- Alice，Bob ともに送信ドメイン認証や S/MIME 等の既存のなりすまし対策は未導入
- Alice，Bob はそれぞれ異なる会社のネットワークに所属し，ネットワーク管理者がそれぞれの会社のネットワーク内の情報通信機器を管理

上記の想定においては通常であれば，攻撃者は Alice になりすましたメールを Bob に送りつけることにより，Bob をマルウェア等に感染させ目的を達成することができる．この時，Canvas フィンガープリントをメールにおける自己証明の認証要素として使用した場合，なりすましメールを防げるか考察する．以後の説明では，認証要素として使用する Canvas フィンガープリントを “F”，メール本文のハッシュ値を “H”，Bob が保持する Alice に関する情報を “F_A” のように表記する．

4.2.1　登録フェーズ

ここでは，Alice が電子メールにおいて身元証明を行うために，Canvas フィンガープリントを利用する状況を想定する．この時，登録フェーズは送受信者それぞれにおいて以下の手順を踏む．

- 送信者（Alice）
  - (1) Thunderbird アドオンにより F を取得
  - (2) 取得した F をネットワーク管理者にメールサーバに登録するように依頼
  - (3) メールサーバでは，Alice のメールアドレスと登録を依頼された F を関連付けて保存
  - (4) ネットワーク管理者は，OS やブラウザのアップデートを行った時に Alice の F を更新登録
- 受信者（Bob）
  - (1) Alice から受信したメールから（F, H）を抽出
  - (2) 抽出した（F, H）を（F_A, H_A）とし，Alice のメールアドレスと関連付けて保存
  - (3) Alice から受信したメールに含まれる F が変化した際は，4.2.2 検証フェーズで示す検証により，信頼された情報であれば更新登録

4.2.2　検証フェーズ

登録フェーズを終えた Alice と Bob がメールでやり取りする状況を想定する．この時，Alice が Canvas フィンガープリント等を付加したメールを Bob 宛に送り，Bob が Canvas フィンガープリントによるなりすましメールの検証を行う手順を以下に示す．

(1) Alice は F と直前に Bob に送信したメールの H を Bob 宛のメールに付与し送信.
(2) Bob は受信メールから（F, H）を抽出し，Alice から直前に受信したメールの（F_A, H_A）と照合し検証を実行
- F だけでなく H についても検証することで，なりすましメールの可能性を低減（攻撃者がなりすましメールを作成するためには，Alice の F 及び H が必要）
- (F, A) と (F_A, H_A) が一致すれば, Alice からのメール.
- F に一致する F_A がない場合，Alice の F が変化，またはなりすましメール
- H が H_A と一致しない場合，なりすましメール

(3) Bob 側において F の検証が失敗した場合，受信したメールの Cc 欄を確認
- Cc 欄に Alice のメールアドレスが含まれていれば, Alice の F が変化した後の最初のメール
- Cc 欄に Alice のメールアドレスが含まれていなければ, なりすましメール, または Alice の Cc 欄記入ミス

(4) Cc 欄に Alice のメールアドレスが含まれていない場合，Alice が所属するネットワークのメールサーバに照合を依頼
- メールサーバにて照合依頼された Alice のメール送信履歴を確認し，真に Alice から Bob 宛にメールが送信されているかを確認．送信履歴が残っていれば，F の変化情報が未共有，または Bob 側での照合ミス
- 送信履歴が無ければ，Bob が受信したメールは Alice のなりすましメール

上記において，送信者の F が変化した場合における送受信者間の情報共有方法についても示した．F が変化した直後のメールにて，Alice が自身のメールアドレスを Cc に含めることで F の変化情報が共有可能である．F が変化した後には Bob にとって新規認証要素になるので，攻撃者が OS のアップデート等により F が変化した Alice と主張すれば Bob には検証する術がないという懸念があった．しかし，提案手法の検証手順により，変化情報の間隙を縫った攻撃者によるなりすましメールを看破できる．もし攻撃者が Alice になりすますメールの Cc に Alice のメールアドレスを含めれば，Alice は送信した覚えのないメールが届くことになるので，なりすましメールは成立しない．また，攻撃者が Cc に Alice のメールアドレスを含めずになりすましメールを Bob に送信した場合，Bob 側と Alice 側メールサーバの検証でなりすましメールに気付くことができる．

5. 考察

4 節において示したように，電子メールにおいて Canvas フィンガープリントを自己の証明手段として利用した場合，今までメールでやり取りしていたユーザのなりすましを看破することが期待できる．フィンガープリントの取得及びなりすまし検証はユーザにとって透過的に実行されるとともに，フィンガープリントが OS やブラウザのバージョンアップに伴い不定期に変化するため，攻撃者にとって推測が困難であるという利点がある．また，フィンガープリントとメール本文のハッシュ値を組み合わせて検証することにより，フィンガープリントを推測または窃取したのみではなりすまし検証をすり抜けできないことを示した．

5.1 提案手法と S/MIME との相違点

提案手法は S/MIME のように，メールに認証要素を付加することによって自己の身元証明を試みる手法である．S/MIME は信頼出来る第三者が発行する電子証明書により身元を証明しているが，提案手法は SYH によって証明を行っている．そのため，S/MIME のように電子署名を外部から取得する必要はなく，ユーザ認証を行うユーザの手元にある環境により認証要素を取得できるので，コストの低減が期待できる．また，S/MIME では Web メールやスマートフォンが対応していないことが多いという問題もあるが，提案手法ではスマートフォンのブラウザから Canvas フィンガープリントを取得できることは確認済みであり，Web ブラウザを使用する Web メールにおいても Canvas フィンガープリントは取得可能であると推察する．

5.2 提案手法の欠点と対応できないなりすましメール

同じ OS，ブラウザ，GPU を使用しているパソコンが複数ある環境においては，フィンガープリントの一意性を確保できない可能性が高い．そのため，Canvas フィンガープリントだけでなく，別の認証要素を組み合わせたフィンガープリントを開発することで，ユーザが所有する端末の一意性を確保する必要がある．また，送信者が使用するフィンガープリントが攻撃者に漏洩した際に，送信者が使用する端末情報推測の足がかりになりかねないという懸念がある．もし攻撃者が複数の OS やブラウザ等を組み合わせた時のそれぞれのフィンガープリント情報を知っており，取得した送信者のフィンガープリントに一致する情報を見つけた場合，その情報をもとにした脆弱性を狙った攻撃に送信者が晒される可能性がある．この対策として，秘密分散を取り入れて端末情報の推測を防ぐ手法や，FIDO のように自らの認証要素を認証情報として送信するのではなく，手元での認証結果を送付するプロトコルが必要になる．

提案手法で対応できないなりすましメールの状況としては，攻撃者によるメール送信端末の乗っ取り，新規メールユーザによるなりすまし，中間者攻撃が挙げられる．端末が乗っ取られた場合の対策としては，SYA によりユーザ自身を認証する手法が考えられる．標的がメールでやり取りをしたことがない新規メールユーザによるなりすましメールでは，受信者が送信者を認証するためのフィンガープリントを持ち得ないので検証ができない．よって，RSA リス

クベース認証 [20] のように複数の認証を準備し，メールのリスクに応じた追加の認証を行う方式が必要であると考える．また，中間者攻撃としてフィンガープリントをそのまま利用されてしまった場合は提案手法では検知できないので，改ざん防止の電子署名が別途必要となる．

6. まとめと今後の課題

電子メールを利用したサイバー攻撃が存在し，その中でも脅威が大きいサイバー攻撃の手口の 1 つとして，なりすましメールがある．なりすましメールには複数の種類があり，既存対策によって対応できる種類が異るが，特に S/MIME はなりすましメールには効果的な対策である．しかし，普及していないという問題が存在する．そこで，S/MIME で使用される電子署名とは別の認証要素について調査し，なりすましメール対策としての有効性について考察した．結果，認証要素の取得が低コストであることやユーザ自身を認証する等の S/MIME とは別の利点を有する認証要素があることを確認できた．調査した認証要素の中でも Canvas フィンガープリントに着目した．提案手法では，特定の条件下で Canvas フィンガープリントとメール本文のハッシュ値を組み合わせた検証を行うことで，なりすましを看破できることについて示した．S/MIME とは別の Canvas フィンガープリントの利点として，ユーザにとって透過的に認証要素の取得検証を行うことができ，不定期にフィンガープリントが変化するため，攻撃者にとって値の推測が困難であること等が挙げられる．また，Canvas フィンガープリントを Thunderbird アドオンにより取得可能であることも確認した．

今後は想定環境で述べた状況を模擬し，Canvas フィンガープリントを取得検証する Thunderbird アドオンを実装することで，提案手法の有効性を実地に確認する．本提案手法では対応できない端末の乗っ取り，新規メールユーザによるなりすましメール及び中間者攻撃に対しては，3 節で検討した他の認証要素や実装手法についても更に研究を深化させていくとともに，改ざん防止手法も調査しなければならない．また，本研究での想定環境では攻撃者による認証妨害については想定対象外としていたため，今後は認証妨害に対する対策についても併せて調査検討していく．

参考文献

[1] 情報処理推進機構,「情報セキュリティ 10 大脅威 2016 〜個人と組織で異なる脅威，立場ごとに適切な対応を〜」, https://www.ipa.go.jp/files/000051691.pdf, 2016 年 8 月 9 日アクセス.

[2] YOMIURI ONLINE,「JTB 個人情報 793 万件流出か?... 標的型攻撃の巧妙な手口」, http://www.yomiuri.co.jp/science/goshinjyutsu/20160615-OYT8T50004.html, 2016 年 8 月 9 日アクセス.

[3] Amin, Rohan Mahesh. “Detecting targeted malicious email through supervised classification of persistent threat and recipient oriented features.” Diss. The George Washington University, 2011.

[4] 一般財団法人日本データ通信協会,「送信ドメイン認証技術導入マニュアル第 2 版」, http://www.dekyo.or.jp/soudan/image/anti_spam/manual/201108MN_all.pdf, 2016 年 8 月 5 日アクセス.

[5] 総務省,「特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況」, http://www.soumu.go.jp/main_content/000354170.pdf, 2016 年 8 月 5 日アクセス.

[6] 総務省,「標的型攻撃に対抗するための通信規格の標準化動向に関する調査結果」, http://www.soumu.go.jp/main_content/000227896.pdf, 2016 年 8 月 5 日アクセス.

[7] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.” Leading Issues in Information Warfare & Security Research 1 (2011): 80.

[8] Kim, Peter. “The hacker playbook2: Practical guide to penetration testing.” Secure Planet LLC, 2015.

[9] Google,「Google 2 段階認証プロセス」, https://www.google.co.jp/intl/ja/landing/2step/, 2016 年 8 月 5 日アクセス.

[10] RSA, “RSA SECURID”, https://www.rsa.com/ja-jp/products-services/identity-access-management/securid, 2016 年 8 月 5 日アクセス.

[11] FIDO Alliance, “Universal 2nd Factor (U2F) Overview”, https://fidoalliance.org/specs/fido-u2f-overview-ps-20150514.pdf, 2016 年 8 月 5 日アクセス.

[12] NTT ドコモ,「生体認証」, https://www.nttdocomo.co.jp/service/bio/index.html, 2016 年 8 月 5 日アクセス.

[13] Lin, Wen-Hui, Ping Wang, and Chen-Fang Tsai. “Face recognition using support vector model classifier for user authentication.” Electronic Commerce Research and Applications (2016).

[14] Karnan, Marcus, Muthuramalingam Akila, and Nishara Krishnaraj. “Biometric personal authentication using keystroke dynamics: A review.” Applied Soft Computing 11.2 (2011): 1565-1573.

[15] De Luca, Alexander, et al. “Touch me once and i know it’s you!: implicit authentication based on touch screen patterns.” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2012.

[16] 情報処理推進機構,「生体認証導入・運用の手引き」, https://www.ipa.go.jp/files/000024404.pdf, 2016 年 8 月 5 日アクセス.

[17] FIDO Alliance, “FIDO UAF Architectural Overview”, https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-overview-v1.0-ps-20141208.pdf, 2016 年 8 月 5 日アクセス.

[18] Mowery, Keaton, and Hovav Shacham. “Pixel perfect: Fingerprinting canvas in HTML5.” Proceedings of W2SP (2012).

[19] Mozilla, “Add-ons”, https://developer.mozilla.org/en-US/Add-ons, 2016 年 8 月 7 日アクセス.

[20] RSA, “Risk-Based Authentication”, https://www.rsa.com/content/dam/rsa/PDF/h13823-ds-rsa-securid-risk-based-authentication.pdf, 2016 年 8 月 8 日アクセス.