情報処理学会論文誌 Vol.60 No.12 2234–2244 (Dec. 2019)

MITB攻撃手法の分類と対策手法の有効性に関する考察

高田 一樹[1,2,a)] 吉岡 克成[3] 松本 勉[3]

受付日 2019年3月11日, 採録日 2019年9月11日

概要：近年，マルウェア感染やフィッシングによってインターネットバンキングの認証情報やクレジットカード情報が盗取されることによる，不正送金や不正利用が社会問題となっている．これらの情報を盗取する攻撃方法の 1 つにマルウェアによる Man-In-The-Browser（MITB）攻撃があり，注目を集めている．MITB 攻撃は，マルウェアが感染 PC の Web ブラウザにプロセスインジェクション等の方法で入り込み通信内容の盗聴や改ざんを行う攻撃手法である．MITB 攻撃によって，インターネットバンキングやクレジットカード会社のサイトとの通信内容が改ざんされ，情報盗取が発生する．我々は，これまで，MITB 攻撃を行う複数のマルウェアを長期的に観測し，攻撃対象・攻撃手法を継続的に分析している．本稿では，MITB 攻撃を行うマルウェアの観測結果に基づき最新の MITB 攻撃手法を体系的に分類し，インターネットバンキングにおいて用いられている既存の対策手法の有効性の検討を行った結果を報告する．また，既存対策における問題点とその対策の検討結果について報告する．

キーワード：MITB 攻撃，インターネットバンキング，不正送金

Taxonomy of MITB Attacks and Analysis on the Effectiveness of Existing Countermeasures

Kazuki Takada[1,2,a)] Katsunari Yoshioka[3] Tsutomu Matsumoto[3]

Received: March 11, 2019, Accepted: September 11, 2019

Abstract: Data theft and fraud financial transfer via phishing websites and malware have become major threats especially for Internet banking and credit card companies. Man-In-The-Browser (MITB) attack is one of the major types of the attack. MITB malware can intercept and tamper communication within the browser. Our analysis is based on long-term observations on various types of MITB malware that targets Japanese companies. As a result, we have revealed various methods and targets of MITB attack. This paper discusses the classification and techniques of MITB attack methods, the effectiveness and problems of existing countermeasures implemented for Internet banking, and make countermeasures more effective.

Keywords: MITB, Internet banking, unauthorized money transfer

1. はじめに

近年，マルウェア感染やフィッシングによってインターネットバンキングの認証情報やクレジットカード情報が盗取されることによる，不正送金や不正利用が社会問題となっている [1]．警察庁によればインターネットバンキングにかかわる不正送金の被害金額は，年々減少傾向にあると報告されているが，2017 年の不正送金の被害は，約 10 億 8,100 万円と依然として多くの被害が発生している [2]．

インターネットバンキングの認証情報やクレジットカー

[1] 横浜国立大学大学院環境情報学府
Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[2] 株式会社セキュアブレイン
SecureBrain Corporation, Chiyoda, Tokyo 102–0094, Japan
[3] 横浜国立大学大学院環境情報研究院/先端科学高等研究院
Graduate School of Environment and Information Sciences, Yokohama National University/Institute of Advanced Sciences, Yokohama National University, Yokohama, Kanagawa 240–8501, Japan
[a)] takada-kazuki-hw@ynu.jp

表 1 分析対象マルウェアの概要
Table 1 Overview of the analysis target malware.

マルウェア（グループ）	主要活動期間	攻撃対象サイト	MITB 攻撃手法		
			コンテンツ改ざん		偽サイト誘導
			情報盗取型	自動送金型	
VAWTRAK	2014.04–2015.07	銀行	✓	✓	
		EC サイト	✓		
		カード会社	✓		
Rovnix	2015.12–2016.06	銀行	✓		
Ursnif および DreamBot（グループ 1）	2016.07–2017.01	銀行	✓		✓
Ursnif および DreamBot（グループ 2）	2017.02–2018.12	銀行	✓	✓	
		カード会社	✓		
		EC サイト	✓		
		Web メール	✓		
		仮想通貨取引所	✓		
		ファイル共有サービス	✓		
Ursnif（グループ 3）	2017.06–2018.12	銀行	✓	✓	✓
		EC サイト	✓		
Ramnit	2018.08–2018.12	カード会社	✓		
		EC サイト	✓		
		Web ポータル	✓		

ド情報を盗取する攻撃方法の 1 つにマルウェアによる Man-In-The-Browser（MITB）攻撃があり，注目を集めている．

我々は，これまでに MITB 攻撃を行う複数のマルウェアに対し，静的解析結果に基づいた長期挙動観測によって，攻撃対象および攻撃手法の分析を継続的に実施している [3]．論文 [3] の調査手法を用いて継続的に観測を行った結果，MITB 攻撃は，攻撃対象をインターネットバンキング以外に拡大し，攻撃手法が高度化していることを明らかにしている．

本稿では，MITB 攻撃を行うマルウェアを長期的に観測を行った結果に基づき，日本国内において 2014〜2018 年の期間に行われた MITB 攻撃手法を体系的に分類した．さらに，分類した各 MITB 攻撃手法に対する，インターネットバンキングにおける既存対策手法の有効性の検討を行った．あわせて，インターネットバンキング以外の攻撃対象における対策状況についても調査を行った．これらの結果および既存対策手法の問題点とその対策の検討結果について報告する．

2. 分析対象マルウェア

本稿では，VAWTRAK，Rovnix，Ursnif，DreamBot，Ramnit の 5 種類のマルウェアの長期観測結果に基づいて MITB 攻撃手法を分類する．これらのマルウェアは，いずれも日本国内においてインターネットバンキングの不正送金やクレジットカード情報の盗取等を引き起こすものとして知られている [4], [5]．

本稿で分析対象とする 5 種類のマルウェアについて**表 1** に示す．各マルウェアとも複数の検体を並行して長期観測している．主要な活動期間は，観測結果に基づくものであるためニュース等で報道されている内容とは異なることがある．表 1 内の MITB 攻撃手法については，3 章に述べる．

表 1 に示すとおり，Ursnif と DreamBot は，攻撃設定情報の復号に使われる RSA の公開鍵および攻撃設定情報に含まれる挿入コード片の内容が共通するものをグルーピングして分析する．（攻撃設定情報は，3.1 節を参照）なお，DreamBot は，Ursnif の亜種であり C&C サーバとの通信に使われるプロトコルの違いを除くと，ほぼ同一の機能を持つマルウェアである．

3. MITB 攻撃

3.1 基本的な MITB 攻撃発生の過程

MITB 攻撃は，マルウェアが感染 PC の Web ブラウザにプロセスインジェクション等の方法で入り込み通信内容の盗聴や改ざんを行う攻撃手法である．MITB 攻撃によって，インターネットバンキング等の攻撃対象サイトとの通信が改ざんされることで情報盗取や不正送金が発生する．

MITB 攻撃は，C&C サーバから配信される攻撃設定情報に従って行われる．攻撃設定情報は，マルウェアによってデータの形式が異なるが，攻撃対象 URL と攻撃手法が設定された情報である．以下に，基本的な MITB 攻撃発生の過程について示す．

1. 感染：スパムメールや不正な Web サイト等を経由してマルウェアに感染する．
2. 攻撃設定情報の取得：マルウェアは，C&C サーバと通信することで，MITB 攻撃の攻撃設定情報を取得する．
3. Web ブラウザ通信の監視：マルウェアは，Web ブラウザの通信を常時監視する．
4. MITB 攻撃発生：Web ブラウザで攻撃対象 URL に接

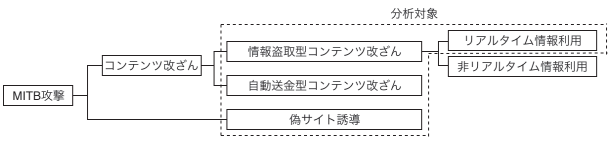

図 1 MITB 攻撃手法の分類
Fig. 1 Taxnomy of MITB attack method.

続すると，MITB 攻撃が発生する．この際，情報盗取や不正送金に利用される不正 JavaScript および偽コンテンツの配信，盗取情報のアップロード先となる攻撃者サーバをマニピュレーションサーバと呼称する．

4. で発生する MITB 攻撃について次節以降で分類を行う．

3.2 MITB 攻撃手法の分類

表 1 の分析対象マルウェアに対して，論文 [3] の手法を用いて行った分析結果に基づき，これらのマルウェアが行う MITB 攻撃を**図 1** のように分類する．図 1 の各攻撃手法は，表 1 の分析対象マルウェアの攻撃設定情報や情報盗取および不正送金に利用される不正 JavaScript の分析，動的解析による MITB 攻撃の再現実験を行った結果に基づいて個々の攻撃手法をモデル化した後に分類を行ったものである．分析対象のマルウェアは，いずれも日本国内において大規模な感染および攻撃を行ったものであり [4], [6], [7], [8], [9]，図 1 に示す分類は，日本国内で発生した主要な MITB 攻撃を分類するものであると考える．

図 1 より，日本国内で発生している主要な MITB 攻撃は，「コンテンツ改ざん」と「偽サイト誘導」の 2 種類に大分される．以下に，それぞれの概要を示す．なお，各 MITB 攻撃手法の詳細については，3.2.1〜3.2.3 項に示す．

なお，図 1 のコンテンツ改ざん攻撃は，論文 [10] 等で分析された海外で発生している MITB 攻撃と同様のものである．また，偽サイト誘導攻撃は，海外で流行した Dyre [11] が同様の MITB 攻撃を行うことが知られている．さらに，我々が Dyre に対して動的解析を用いて調査した結果，偽サイト誘導攻撃を行うことを確認している．このように，本研究の分類結果は，日本国内だけでなく国際的に共通して適用可能であると考えられる．一方，MITB 攻撃には，ユーザが送金手続きを行った際に，ブラウザとインターネットバンキングシステムとの通信内容のうち送金先や送金金額の情報を改ざんして不正送金を行う攻撃方法の存在が知られている．我々の調査した範囲では，2014.04〜2018.12 までの間に，送金情報の書き換え攻撃を行うマルウェアの流行が確認されていないため本研究における分類の対象外とする．

(1) コンテンツ改ざん

コンテンツを改ざんすることにより，情報盗取や自動的に送金する機能を持つ不正な JavaScript を読み込ませる．攻撃設定情報には，攻撃対象 URL と改ざん対象文字列および改ざん時に挿入される不正コード（挿入コード片）が設定されており，攻撃対象 URL に接続をするとコンテンツに挿入コード片を挿入する．挿入コード片は，不正 JavaScript を読み込むための Script タグ等を含んでいる．挿入コード片が Web ブラウザで実行されることによって，不正 JavaScript を外部サーバから読み込ませる．

コンテンツ改ざんは，用いられる不正 JavaScript の機能に基づき，以下の 2 種類が存在する．

- 情報盗取型コンテンツ改ざん
- 自動送金型コンテンツ改ざん

表 1 に示すとおり，情報盗取型コンテンツ改ざんは，すべての分析対象マルウェアにおいてすべての攻撃対象サイトに対して確認された攻撃手法である．自動送金型コンテンツ改ざんは，VAWTRAK，Ursnif および DreamBot（グループ 2），Ursnif（グループ 3）で確認された攻撃手法である．なお，Ursnif（グループ 3）でのみ通信先の一部を改ざんすることであらかじめ挿入コード片を埋め込んだコンテンツを読み込ませて，不正 JavaScript を外部サーバから読み込ませる攻撃が行われる．これは，最終的に発生する攻撃が同一であるため，マルウェアが挿入コード片をコンテンツに挿入する改ざん方法に含まれるものとする．

(2) 偽サイト誘導

Web ブラウザから発生する通信先を変更することで，コンテンツのすべてを入れ替える．攻撃設定情報には，攻撃対象 URL と置換後の URL が設定されており，攻撃対象 URL に接続すると通信先を置換する．なお，この際に，置換前の URL との接続や証明書検証結果の改ざんを行う．これによって，Web ブラウザのアドレスバーの証明書情報を正規の内容としたり，証明書エラーを回避することを確認している．偽サイト誘導は，中間者攻撃の一種とも考えられるが，本稿ではマルウェアによってブラウザ内で通信先が改ざんされる MITB 攻撃としてとらえる．表 1 に示すとおり，偽サイト誘導攻撃は，Ursnif および DreamBot（グループ 1）および Ursnif（グループ 3）で確認された攻撃手法である．

3.2.1 情報盗取型コンテンツ改ざん攻撃

図 2 は，情報盗取型コンテンツ改ざん攻撃の攻撃順序をモデル化したものである．なお，分析対象マルウェアで用いられる銀行を攻撃対象とする不正 JavaScript を調査した結果，マニピュレーションサーバ側で盗取した情報をリアルタイムに利用していると思われる機能が実装されているものの存在を Ramnit を除くすべての分析対象マルウェアで確認した．これは，不正 JavaScript がマニピュレーションサーバにコンテンツ改ざんの状態を通知し，マニピュレーションサーバから指示を受けて次の動作を決定する機能である．この機能によって，送金時の決済認証にワンタイムパスワード（以下，OTP）等を利用する銀行で不正送金を可能としていた．この機能を考慮したものが，図 2 の

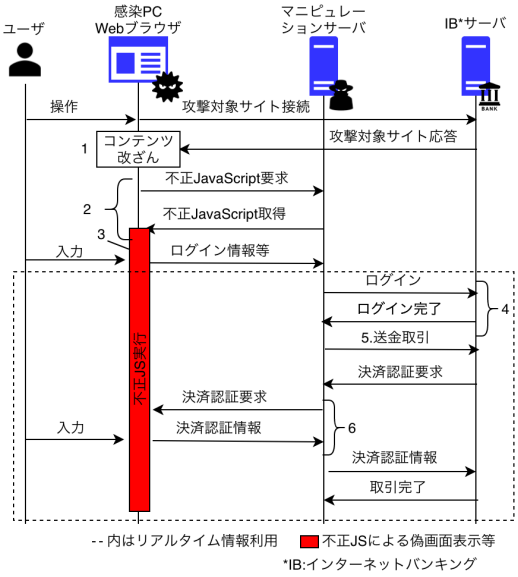

図 2 情報盗取型コンテンツ改ざん攻撃モデル

Fig. 2 Model of information stealing type contents tampering attack.

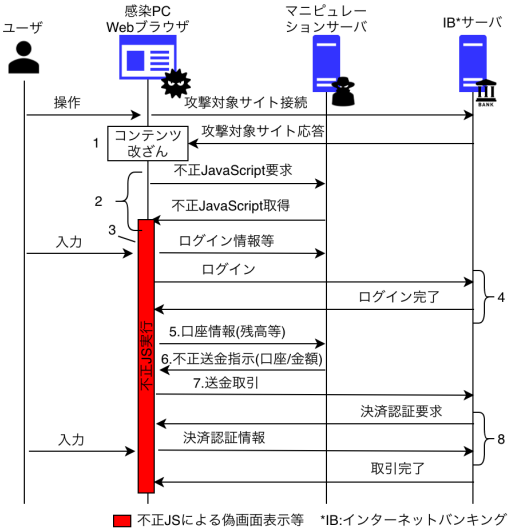

図 3 自動送金型コンテンツ改ざん攻撃モデル

Fig. 3 Model of auto transfer type contents tampering attack.

リアルタイム情報利用時のモデルである．図 2 に示すとおり，情報盗取型コンテンツ改ざん攻撃は，以下の順序で行われる．リアルタイム情報利用時には，4〜6 に示す攻撃が発生すると想定される．非リアルタイム情報利用は，固定的な ID，パスワード等でのみ認証を行っている場合に行われる攻撃で，3 のタイミングで必要な情報を盗取し，攻撃者は盗取した情報を任意のタイミングで利用可能である．

1. コンテンツ改ざん：ユーザが攻撃対象サイトに接続すると，マルウェアによって改ざん対象コンテンツに挿入コード片が挿入される．

2. 不正 JavaScript の取得：挿入コード片が実行され，マニピュレーションサーバから不正 JavaScript が取得される．

3. 不正 JavaScript の実行：不正 JavaScript が実行されることで，ユーザの入力した ID，パスワードやコンテンツに含まれる情報の盗取が発生する．また，情報を盗取するための偽画面を表示することもある．

4. 盗取情報による不正ログイン：盗取したログイン情報を利用してリアルタイムで攻撃者が不正ログインをする．

5. 不正送金取引：不正ログイン完了後に，送金取引を行う．

6. 決済認証情報の盗取：マニピュレーションサーバから不正 JavaScript に指令して，ログインに必要な情報を装う偽画面で OTP 等の送金決済認証情報を盗取する．

なお，2018.12 時点で，銀行に対するリアルタイム情報利用が行われると思われる攻撃対象は，Ursnif および DreamBot（グループ 2）で 40%（不正 JavaScript 10 ファイル中，4 ファイル），Ursnif（グループ 3）で 100%（不正 JavaScript 2 ファイル中，2 ファイル）であった．Ursnif および DreamBot（グループ 2）では，60%が第 2 暗証番号等の固定的な決済認証情報を盗取するものであったが，これは攻撃対象の銀行がリアルタイム情報利用を必要としない決済認証情報を利用しているためである．残り 40%のリアルタイム情報利用が行われる攻撃対象の銀行は，OTP 等による決済認証情報の利用が必須または強く推奨されていた．今後，固定的な決済認証情報から OTP 等の決済認証情報への移行がさらに進むことが考えられるが，その結果，MITB 攻撃の対象外となるのではなく，リアルタイム情報利用が用いられる可能性が高いと考えられる．

3.2.2 自動送金型コンテンツ改ざん攻撃

情報盗取型コンテンツ改ざん攻撃では，盗取した情報を不正利用している．これに対し，自動送金型コンテンツ改ざん攻撃は，感染 PC の Web ブラウザから不正 JavaScript が送金取引を行う攻撃である．

図 3 は，自動送金型コンテンツ改ざん攻撃の攻撃順序をモデル化したものである．図 3 に示すとおり，自動送金型コンテンツ改ざん攻撃は，以下の順序で行われる．

1. コンテンツ改ざん：ユーザが攻撃対象サイトに接続すると，マルウェアによって改ざん対象コンテンツに挿入コード片が挿入される．

2. 不正 JavaScript の取得：挿入コード片が実行されマニピュレーションサーバから不正 JavaScript が取得される．

3. 不正 JavaScript の実行：不正 JavaScript が実行されることで，ユーザの入力した ID，パスワードやコンテンツに含まれる情報の盗取が発生する．また，情報を盗取するための偽画面を表示することもある．

4. ログイン：インターネットバンキングにログインする．この際，不正 JavaScript が偽画面等を表示して未ログイン状態を装う．

5. 口座情報の収集：口座情報（口座番号，残高等）をマニピュレーションサーバにアップロードする．

6. 不正送金指示：送金先の口座情報および送金金額等の不

正送金に必要な情報を不正 JavaScript に指示する．

7. 不正送金取引：不正 JavaScript がインターネットバンキングシステムと通信し，送金取引を行う．

8. 決済認証情報の盗取：不正 JavaScript がログインに必要な情報を装う偽画面で OTP 等の送金決済認証情報を盗取する．

3.2.3 偽サイト誘導攻撃

偽サイト誘導攻撃は，攻撃対象 URL に接続した際にすべてのコンテンツ取得通信先を攻撃者のサーバに変更することで偽サイトに誘導するものである．

2018.12 時点で偽サイト転送が行われる Ursnif（グループ 3）の攻撃対象の 4 つの銀行は，いずれも送金時の決済認証に OTP を利用するものであった．さらに，偽サイトで用いられる JavaScript を調査した結果，4 つの銀行すべてに対して OTP を盗取する実装がなされていた．このことから，情報盗取型コンテンツ改ざん攻撃と同様にリアルタイムに盗取した情報を利用していると考えられる．

図 4 は，偽サイト誘導攻撃の攻撃順序をモデル化したものである．図 4 に示すとおり，偽サイト誘導攻撃は，以下の順序で行われる．

1. 通信先改ざん：ユーザが攻撃対象サイトに接続すると，マルウェアによって通信先が改ざんされ偽サイトへ誘導される．

その際，一部の改ざん前の通信先への接続や証明書の検証結果を改ざんすることで，正規サイトへの接続偽装や証明書エラーの回避が行われる．

2. ログイン：偽サイトに対しユーザがログイン等の操作を行うことにより，情報が盗取される．

3. 盗取情報による不正ログイン：盗取したログイン情報を利用してリアルタイムで攻撃者が不正ログインをする．

4. 不正送金取引：不正ログイン完了後に残高，送金決済認証方法等を確認したうえで不正送金取引を行う．

5. 決済認証情報の盗取：偽サイト上で，ログインに必要な情報を装う偽画面で OTP 等の送金決済認証情報を盗取する．

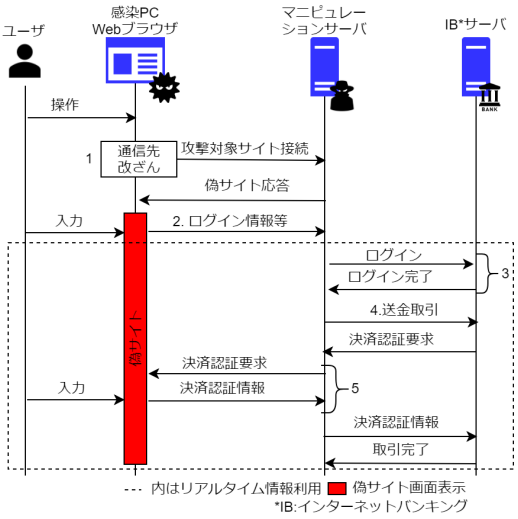

図 4 偽サイト誘導攻撃モデル

Fig. 4 Model of fake site induction attack.

3.3 MITB 攻撃手法と攻撃対象の関係性

各 MITB 攻撃手法と攻撃対象の関係性を整理する．**表 2** に，各攻撃対象に対して用いられる攻撃の最終目的と MITB 攻撃手法の関係をまとめる．

表 2 から，銀行を攻撃対象とする場合，3 種類すべての攻撃手法が用いられる．情報盗取型コンテンツ改ざん攻撃は，リアルタイム情報利用と，非リアルタイム情報利用の 2 種類が存在する．分析の結果，リアルタイム情報利用は銀行に対してのみ利用され，非リアルタイム情報利用は，銀行を含むすべての攻撃対象に対して利用されていることを確認した．銀行に対する対策手法の有効性の検討においては，3.2.1 項で述べたとおり，今後，リアルタイム情報利用が用いられる可能性が高いためリアルタイム情報利用のみを検討対象とする．また，偽サイト誘導攻撃の攻撃対象は，3.2.3 項で述べたとおり，2018.12 時点では，すべての攻撃対象にリアルタイム情報利用が用いられるため，リアルタイム情報利用のみを想定する．

3.4 MITB 攻撃と連携するマルウェア機能の考慮

分析対象マルウェアは，いずれも MITB 攻撃以外の攻撃機能を有しているが，本稿においては，MITB 攻撃以外の機能は基本的に分析対象とはしない．しかし，Ursnif および DreamBot で用いられるコンテンツ改ざんまたは偽サイ

表 2 攻撃対象ごとの最終目的と MITB 攻撃手法

Table 2 Relationship between final purpose against attack target and MITB attack method.

攻撃対象	最終目的	MITB 攻撃手法
銀行	不正送金	情報盗取型（リアルタイム），自動送金型，偽サイト誘導
カード会社	クレジットカード情報盗取	情報盗取型（非リアルタイム）
EC サイト		
Web ポータル		
仮想通貨取引所	仮想通貨送金	
ファイル共有サービス	認証情報盗取	
Web メール	メールアドレス情報盗取	

ト誘導以外の機能のうち以下の機能については，MITB 攻撃との連携を考慮する必要があると考える．

VNC 機能：攻撃対象 URL に接続した際，VNC モジュールをダウンロードして，起動する．

VNC 機能は，感染 PC を遠隔操作することが可能であり，銀行を狙った情報盗取型コンテンツ改ざん攻撃や偽サイト誘導攻撃とあわせて設定されることを確認している．このため，対策手法の有効性の検討においては，VNC 機能があわせて用いられるケースを考慮する必要がある．なお，この際に用いられる VNC 機能は，Hidden VNC [12] と呼ばれる方法が用いられ，感染 PC 上で利用者が遠隔操作に気づくことはできない．

4. 既存対策手法の有効性の検討

各 MITB 攻撃モデルに対して，インターネットバンキングにおける個々の既存対策手法の有効性について検討を行った結果について述べる．あわせて，銀行以外の企業における MITB 攻撃対策の状況について調査を行った結果について述べる．

4.1 対策手法

本稿では，インターネットバンキングにおける既存の対策手法として，全国銀行協会の文献 [13], [14] の「銀行が講じるセキュリティ対策事例」で紹介されている内容を参照する[*1]．対策手法を**表 3** に示す．表 3 から対策手法は，認証系，検知系，運用系の 3 種類に分けられる．このうち，運用系は，MITB 攻撃に対する直接の対策ではないため，認証系，検知系の項目を検討の対象とする．

認証系対策は，インターネットバンキングへのログインや決済認証を強化するものである．OTP は，ハードトークンやスマートフォンアプリを利用した使い捨て PIN コードの発行，2 経路認証は，メールや SMS 等の経路を利用した OTP の発行を想定している．また，トランザクション認証は，ハードトークンを利用し，送金処理の際にハードトークンに取引内容（送金先口座番号等）を入力して Transaction Authentication Number（以下，TAN）を生成し，生成した TAN を用いた決済認証を行う方式を想定している．

検知系対策は，マルウェア感染を検知する専用のウィルス対策ソフトの配布や，改ざん検知製品の導入である．改ざん検知製品は，インターネットバンキングのコンテンツと Web ブラウザ上の DOM 情報等を検査する JavaScript を同時に配信し，検査結果をインターネットバンキングサーバに通知することでコンテンツ改ざん等を検知し，取引の停止やユーザへの警告を行うシステムを指す [16], [17].

[*1] 対策手法の調査は，論文 [15] の検討方法を参考とした．

表 3 対策手法
Table 3 Existing countermeasure.

認証系	OTP，2 経路認証，リスクベース認証，トランザクション認証，電子証明書（ハードトークン）*
検知系	専用ウィルス対策ソフト，改ざん検知製品
運用系	不正ログイン・不正取引のモニタリング，当日送金の制限*

*法人口座のみ

表 4 各 MITB 攻撃手法に対する対策手法の有効性
Table 4 Effectiveness of existing countermeasure against each MITB attack method.

	MITB 攻撃手法		
対策手法	情報盗取型	自動送金型	偽サイト誘導
OTP	×	×	×
2 経路認証	×	×	×
リスクベース認証	×	×	×
トランザクション認証	○	○	○
電子証明書	○*	×	○*
専用ウィルス対策ソフト	○	○	○
改ざん検知	○	○	×

○：対策が有効，×：対策が無効
*VNC による遠隔操作と連携した場合は “×”

4.2 対策手法の有効性

それぞれのセキュリティ対策が各 MITB 攻撃手法に対して有効であるかを検討した結果を**表 4** に示す．

従来から用いられる OTP，2 経路認証，リスクベース認証は，すべての MITB 攻撃手法に対して有効ではない．MITB 攻撃では，盗取した情報をリアルタイムで利用する攻撃を行うため OTP や 2 経路認証を盗取することが可能である．具体的には，情報盗取型改ざん攻撃の図 2 における 6. 決済認証情報の盗取，自動送金型コンテンツ改ざん攻撃の図 3 における 8. 決済認証情報の盗取，偽サイト誘導攻撃の図 4 における 5. 決済認証情報の盗取に示したように，攻撃者が決済認証情報を利用する時点で OTP や 2 経路認証等の決済認証情報を偽画面等で盗取する方法が用いられる．リスクベース認証は，固定的な情報を設定する方式である．このため，攻撃者はあらかじめどのような認証情報が設定可能であるかを調査することで，認証情報盗取画面を作成し盗取することが可能である．具体的には，情報盗取型改ざん攻撃および偽サイト誘導攻撃では，ユーザの入力するログイン情報に加えて偽のリスクベース認証画面を表示することで盗取する方法が用いられる．なお，自動送金型コンテンツ改ざん攻撃では，ユーザが感染 PC 上でログイン操作を行うためリスクベース認証が必要な場合，ユーザ自身が認証を行うため無効化されてしまう．

トランザクション認証は，決済認証情報であるため各

MITB 攻撃手法を用いて OTP や 2 経路認証と同様のタイミングで盗取を行うことが可能である．しかし，トランザクション認証は，感染 PC 以外の専用ドングル等で送金処理の内容を確認して認証する方式であるためユーザ自身が行っていない送金処理の認証であることに気づき処理を中断すると考えられる．よって，すべての MITB 攻撃手法に対して有効と考えられる．

電子証明書は，自動送金型コンテンツ改ざん攻撃では，利用者がインターネットバンキングを行っている感染 PC 上で送金が行われる．よって，電子証明書がセットされた正規の状態を悪用される形で無効化されてしまう．情報盗取型コンテンツ改ざん攻撃および偽サイト誘導攻撃の場合，電子証明書がないため攻撃者の環境から不正ログインが行えないため対策として有効であると考えられる．しかし，3.4 節で述べた VNC 機能を用いることで，インターネットバンキング操作中の感染 PC を VNC 機能で遠隔操作し，図 2 および図 4 内のマニピュレーションサーバからインターネットバンキングに行われる不正なログイン等の操作を感染 PC 上で行うことで無効化されてしまう．

専用ウィルス対策ソフトは，MITB 攻撃を行うマルウェアそのものを検知するためすべての MITB 攻撃手法に対して有効と考えられる．改ざん検知製品は，正規コンテンツ内に自身の改ざんを検知する仕組みを内包するものであるため，情報盗取型改ざん攻撃および自動送金型コンテンツ改ざん攻撃では，図 2 および図 4 内の 1. コンテンツ改ざんや 3. 不正 JavaScript の実行によるコンテンツの変化を検知することが可能であるため有効と考えられる．しかし，偽サイト誘導をされると正規のインターネットバンキングサイトに接続しないため改ざん検知製品の仕組みが無効化されてしまう．

4.3 銀行以外の MITB 攻撃対策の実態

銀行では，既存対策手法を用いた MITB 攻撃を含む不正送金への対策が積極的に行われている [18]．本稿では，銀行以外の攻撃対象における MITB 攻撃対策の実態を調査した．調査は，分析対象マルウェアのいずれかの攻撃設定情報に含まれたことのある，カード会社 12 社，仮想通貨取引所 5 社，EC サイト 2 社，Web ポータル 2 社，Web メール 2 社，ファイル共有サービス 1 社のログイン画面に接続し，MITB 攻撃に関する警告表示および専用ウィルス対策ソフト配布等の有無を確認した．その結果，MITB 攻撃に関する警告表示はカード会社 4 社で，専用ウィルス対策ソフト配布はカード会社 1 社でのみ行われるという状況であった．

仮想通貨取引所では，不正ログイン等の対策として 2 経路認証の利用が推奨されている．しかし，2 経路認証の利用が必須となっているのは，攻撃対象の 5 社中 1 社のみであり，他 4 社は利用者が選択する形になっていた．

5. 考察

4 章をふまえ各対策手法のメリット・デメリットを整理し，各対策手法を利用するうえでの問題点とその対策について考察した結果を報告する．

5.1 既存対策手法の問題点と対策

4.2 節の結果から，すべての MITB 攻撃手法に対して有効な対策手法は，トランザクション認証および専用ウィルス対策ソフトの 2 種類である．これらの対策手法を利用するうえでの問題点およびその対策について考察する．

また，無効であると判断した対策手法についても同様にその問題点と対策について考察する．

5.1.1 有効と判断した対策手法の問題点と対策

(1) トランザクション認証

トランザクション認証は，送金内容を認識して認証する方式のため不正送金に対して有効である．しかし，トランザクション認証であっても不正送金が発生する可能性が存在する．

それは，トランザクション認証の際に何を認証しているのかを正確に確認できない場合である．例として，電卓型のハードトークンを用いるような場合，送金先口座番号や送金金額等を入力して認証を行う．しかし，利用者が何を入力しているのか正確に把握していない場合は，MITB 攻撃による偽画面等でハードトークンの操作を促されると誤って不正送金を認証してしまう可能性がある．この問題は，認証の内容を正確に視認可能なハードトークンやスマートフォンアプリを利用することで対策が可能である．また，トランザクション認証について利用者に正しく理解してもらうことで誤操作を防ぐというアプローチも考えられる．

トランザクション認証は，決済認証を強化する方法であるため，MITB 攻撃によってログイン認証情報が盗取されてしまうことに対する対策にはならない．ログイン認証情報が盗取されることにより，インターネットバンキングに登録されている個人情報や残高等資産情報の流出等の被害が考えられる．このため，検知系の対策により，感染 PC でインターネットバンキングを利用することを未然に防止する等の対策が必要である．

トランザクション認証の導入には，システムの大幅な変更やハードトークンの配布等，導入コストが高いことが想定されるため導入自体が難しいことが懸念される．しかし，トランザクション認証は，不正送金に対して最も効果的な対策であると考えられるため可能な限り，すべての金融機関で導入されることが望ましい．

(2) 専用ウィルス対策ソフト

専用ウィルス対策ソフトの導入は，MITB 攻撃を行うマルウェア自体を検知するため MITB 攻撃に対して有効であ

る．しかし，専用ウィルス対策ソフトは，アンチウィルスソフトの一種であるためすべてのマルウェアを検知可能とは限らない点に注意が必要である．また，すべての利用者がインストールするとは限らない．別のアンチウィルスソフトとの競合や利用環境の問題でインストールが行えない利用者も存在するためインストールを強制することは困難であると考えられる．よって，検知漏れやインストールしていないユーザが存在することをふまえて，ログイン認証および決済認証の強化をあわせて行う必要がある．また，専用ウィルス対策ソフトを導入していない利用者に対するモニタリングの強化や送金の制限等による不正送金の防止および専用ウィルス対策ソフトの導入を促すといったことも考えられる．なお，利用者に対して，専用ウィルス対策ソフトの導入および推奨利用環境の利用を促す活動は継続的に行う必要がある．

5.1.2 無効と判断した対策手法の問題点と対策

(1) OTP および 2 経路認証

OTP，2 経路認証は，リアルタイムで情報利用する必要があるため盗取の手法は，4.2 節で述べたとおり，トランザクション認証と同様である．このため，固定的な ID・パスワードによる認証に比して堅牢であるといえる．これらの決済情報が盗取される原因としては，利用者が決済認証情報をどのように利用するかを正確に把握していないためであると考えられる．よって，トランザクション認証と同様に認証情報の利用方法を利用者に正しく理解してもらうことによって盗取を防ぐというアプローチが考えられる．しかし，何を認証しているのかを利用者が正確に認識可能なトランザクション認証の方が利用者が理解しやすいため，より有効であると考えられる．また，OTP，2 経路認証は，決済認証であるためトランザクション認証と同様に不正送金に対する対策であり，ログイン情報の盗取に対しては，検知系の対策とあわせて用いる必要がある．なお，2 経路認証では，メール，SMS 等で OTP を送付する際に何の認証を行うかの詳細を記載することでトランザクション認証と同等の効果を得ることが可能であると考える．しかし，感染 PC 上で 2 経路認証のメールを受信するような場合は，マルウェアによってメールの内容を盗聴される可能性がある．また，攻撃者がログイン後に通知先のメールアドレスを変更することで 2 経路認証を無効化することも想定される．よって，2 経路認証は，スマートフォン等の感染 PC とは別経路で通知が行われ，通知先を安易に変更できない運用が望ましい．

(2) リスクベース認証

リスクベース認証は，固定的な認証情報を設定する方式であるため MITB 攻撃による盗取が容易であり，MITB 攻撃において不正ログインを防止する手法とはいえない．しかし，リスクベース認証は，利用者が定常的に使用している環境以外であることを検知した際に用いられる．よって，リスクベース認証が有効となった時点でシステム運用者が不正利用の可能性を考慮してモニタリング対象とする等の運用を行うことで不正送金のリスクが低減されると考える．

(3) 電子証明書（ハードトークン）

電子証明書は，自動送金型コンテンツ改ざん攻撃や VNC 機能と連動した際の情報盗取型コンテンツ改ざん攻撃および偽サイト誘導攻撃に対して有効ではないと判断した．しかし，電子証明書が感染 PC にセットされている状態のみで攻撃可能である．よって，電子証明書の適切な運用を行うことで MITB 攻撃によってログイン認証情報が盗取された際に継続して攻撃者によるログインを行わせないといった点での効果は期待できる．しかし，電子証明書は遠隔操作に対して脆弱であるため，不正送金対策としては，トランザクション認証等の決済認証と併用して用いる必要がある．たとえば，電子証明書がセットされていれば，送金等の決済も行えるといったシステム運用は避けるべきである．

(4) 改ざん検知製品

改ざん検知製品は，MITB 攻撃によるコンテンツ改ざんを検知するため偽サイト転送型攻撃に対して有効ではない．これは，コンテンツ改ざんを検知する仕組みがコンテンツ内に内包されていないサイトに誘導されるため対策が困難である．しかし，情報盗取型コンテンツ改ざん攻撃や自動送金型コンテンツ改ざん攻撃には有効であり，コンテンツ内に検知の仕組みを内包するため同じ検知系対策である専用ウィルス対策ソフトとは異なり，利用者すべてをカバー可能という利点がある．改ざん検知製品は，専用ウィルス対策ソフトの導入を行わない利用者にも検知系対策を適用するための補完手法としてとらえる必要があると考えられる．なお，改ざん検知系製品は，無効化されるケースに加え，専用ウィルス対策ソフトと同様に検知漏れが発生する可能性があるためログイン認証および決済認証の強化をあわせて行う必要がある．

5.2 既存対策手法の活用方法

4.2 節および 5.1.1 項の結果から MITB 攻撃による不正送金対策には，トランザクション認証および専用ウィルス対策ソフトが最も有効であることを確認した．また，それぞれの問題点と対策を検討することで有効的な利用方法について考察した．また，無効と判断した対策についても同様の検討を行った．

これらの結果から，MITB 攻撃による不正送金対策は，その効果を理解したうえで，複数の対策手法を組み合わせた運用を行う必要があると考える．対策手法を組み合わせる利用方法としては，検知系の対策，認証系のログイン認証強化，決済認証強化を組み合わせて使用することが重要である．検知系の手法で MITB 攻撃を未然に防止したうえで，検知が行えない攻撃に対し電子証明書による不正ログ

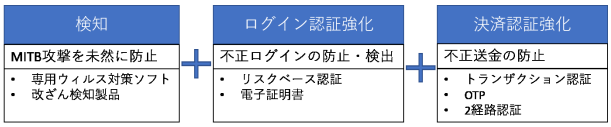

図 5 対策手法の組合せ
Fig. 5 Multiple countermeasure.

インの防止やリスクベース認証による不正ログインの可能性の検出，トランザクション認証等の決済認証情報による不正送金の防止という，検知，ログイン認証強化，決済認証強化という 3 つを組み合わせることが重要であると考える（**図 5**）．また，各対策手法と運用による対策の連携も重要である．

加えて，サービスの運用者だけでなく，利用者も攻撃手法および対策手法について理解を深めることで，対策の効果が発揮されると考える．現在，銀行をはじめ，多くの関係機関が絶えず不正送金に対する啓蒙活動を行っているが，利用者側も積極的に知ろうとする意識が必要であると考える．

4.3 節の結果より銀行以外の攻撃対象では，MITB 攻撃対策が積極的に行われていないことが分かった．仮想通貨取引所は，今後，被害が増大した場合，銀行と同様の不正送金対策が求められる可能性がある．その際には，本稿を含む MITB 対策の研究を参考に対策について十分に検討することが望ましい．カード会社等の攻撃対象では，情報盗取自体が目的となるため検知系対策が主体となると考えられる．しかし，クレジットカード情報の盗取は，カード会社以外のサイトも攻撃に利用されているためカード会社のみで対策を徹底することは困難である．そのため，国等が主体となって MITB 対策・検知の仕組みをすべての企業や利用者に行きわたらせる必要があると考える．

6. 関連研究

MITB 攻撃による不正送金の手法および対策の分析を行った研究について述べる．鈴木らの論文 [19] では，MITB 攻撃を ID 盗取型 MITB 攻撃と取引改ざん型 MITB 攻撃に分類し，MITB 攻撃対策として取引認証方式を導入することによる安全性について評価を行っている．佐野らの研究 [20] では，不正送金について分析を行い，中でも MITB 攻撃に注目して対策の必要性を報告している．岡田らの研究 [21] では，ID 盗取型 MITB 攻撃と取引改ざん型 MITB 攻撃について不正送金対策のための金融サイバーキルチェーン（以下，CKC）を構築し，金融 CKC の各段階において必要な対策の検討を行っている．

これらは，いずれも過去の一般的な MITB 攻撃から想定される攻撃方法に対して，対策手法の検討を行ったものである．これらの研究で検討されている ID 盗取型 MITB 攻撃は，本稿における情報盗取型コンテンツ改ざん攻撃と同様であると考えられる．情報盗取型コンテンツ改ざん攻撃において，これらの論文では言及されていないリアルタイム情報利用を含むモデル化を行っている点で異なっている．また，これらの論文では述べられていない，自動送金型コンテンツ改ざん攻撃および偽サイト誘導攻撃のモデル化を行っている点も異なっている．さらに，MITB 攻撃と連動する VNC 機能を考慮に入れた攻撃の分析も実施している．このように，本稿では，これまで考慮されてこなかった攻撃を含む対策手法の有効性を検討することを可能とした．なお，本稿では，分析対象マルウェアの行う攻撃手法の分析に基づいており，分析期間に確認されなかった取引改ざん型 MITB 攻撃については検討を行っていない．

岡林らの論文 [15] では，インターネットバンキングに対して行われる不正送金攻撃をモデル化することで被害金額を推定し，対策の導入によって，どの程度，被害金額が減少するかを検討している．本稿では，MITB 攻撃手法に対する対策の有効性を検討することを目的としており，有効性の分析の観点が異なっている．

Kiwia らの論文 [22] では，CKC に基づく Banking Trojan の分類法を提案している．論文 [22] では，Banking Trojan の感染手法や攻撃機能を CKC の適用するステップに当てはめた脅威分析モデルを構築し，英国の金融機関を標的とする Banking Trojan の分類を試みている．また，CKC を用いることで，分類した Banking Trojan に対して，CKC の各ステップで用いられるべき対策手法を適切かつ容易に検討することが可能となるとしている．論文 [22] は，CKC による Banking Trojan の分類および，それによって対策手法の検討を容易にすることを主な目的としている．本稿では，複数のマルウェアによる MITB 攻撃を分析した結果から MITB 攻撃手法を分類しモデル化している．また，MITB 攻撃に対する既存対策手法の有効性について検討を行っており，研究の目的が異なっている．

Continella らの Prometheus [23] では，MITB 攻撃によるコンテンツ改ざんを検知基盤で検知することやセキュアなインターネットバンキング環境の提供を最終目的として，動的解析を用いた検知技術の研究をしている．本稿では，MITB 攻撃に対して，既存の対策技術の有効性について検討を行っており，研究の目的が異なっている．

7. まとめと今後の課題

本稿では，2014〜2018 年にかけて日本国内で行われている MITB 攻撃手法を分類してモデル化した．また，各 MITB 攻撃手法に対し，既存の対策手法の有効性の検討を行った．その結果として，金融機関は，既存対策を組み合わせた運用と利用者への適切な啓蒙活動が必要であると結論付ける．今後，MITB 攻撃手法に対するより有効な対策手法および対策を行きわたらせる仕組みについて検討する．

謝辞 本研究成果の一部は，国立研究開発法人情報通信

研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」によって得られた．

参考文献

[1] 独立行政法人情報処理推進機構セキュリティセンター：情報セキュリティ 10 大脅威 2019（オンライン），入手先 ⟨https://www.ipa.go.jp/security/vuln/10threats2019.html⟩（参照 2019-02-05）．

[2] 警察庁：平成 29 年中におけるサイバー空間をめぐる脅威の情勢等について（オンライン），入手先 ⟨https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_cyber_jousei.pdf⟩（参照 2018-11-28）．

[3] 高田一樹，岩本一樹，遠藤　基，奥村吉生，岡田晃市郎，西田雅太，吉岡克成，松本　勉：静的解析と挙動観測を組み合わせた金融マルウェア長期観測手法の提案，情報処理学会論文誌，Vol.59, No.12, pp.2087–2104 (2018).

[4] トレンドマイクロ：日本で猛威を振るう「VAWTRAK」とは（オンライン），入手先 ⟨https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/web-attack/3141/vawtrak-plagues-users-in-japan⟩（参照 2018-12-03）．

[5] 一般社団法人日本サイバー犯罪対策センター：マルウェア情報（オンライン），入手先 ⟨https://www.jc3.or.jp/info/malware.html⟩（参照 2018-12-03）．

[6] トレンドマイクロ：狙いは国内ネットバンキング，日本郵政を騙るマルウェアスパムが拡散（オンライン），入手先 ⟨https://blog.trendmicro.co.jp/archives/12884⟩（参照 2019-06-14）．

[7] 一般社団法人日本サイバー犯罪対策センター：インターネットバンキングマルウェア「Gozi」による被害に注意（オンライン），入手先 ⟨https://www.jc3.or.jp/topics/gozi.html⟩（参照 2019-06-14）．

[8] 一般社団法人日本サイバー犯罪対策センター：インターネットバンキングマルウェア「DreamBot」による被害に注意（オンライン），入手先 ⟨https://www.jc3.or.jp/topics/dreambot_cm.html⟩（参照 2018-12-03）．

[9] トレンドマイクロ：クレジットカード情報を狙うウイルス「RAMNIT」が，日本にも本格上陸（オンライン），入手先 ⟨https://is702.jp/news/2163/⟩（参照 2019-06-14）．

[10] Boutin, J.-I.: The Evolution of Webinjects, *Virus Bulletin Conference*, pp.25–34 (2014).

[11] シマンテック：金融機関を狙うトロイの木馬として主力となった Dyre（オンライン），入手先 ⟨https://www.symantec.com/connect/nl/blogs/dyre?page=1⟩（参照 2019-06-14）．

[12] 吉川孝志，菅原　圭：隠された（見えない）デスクトップに潜む脅威とその仕組み，MBSD Blog（オンライン），入手先 ⟨https://www.mbsd.jp/blog/20180914.html⟩（参照 2019-06-25）．

[13] 全国銀行協会：インターネット・バンキングにおけるセキュリティ対策事例（オンライン），入手先 ⟨https://www.zenginkyo.or.jp/fileadmin/res/news/news280614_1.pdf⟩（参照 2018-12-05）．

[14] 全国銀行協会：銀行および法人のお客さまに求められるセキュリティ対策事例（オンライン），入手先 ⟨https://www.zenginkyo.or.jp/fileadmin/res/news/news260717_1.pdf⟩（参照 2018-12-05）．

[15] 岡林喬久，猪俣敦夫：インターネットバンキングにおける不正送金被害額の推定，情報処理学会論文誌，Vol.58, No.12, pp.1935–1942 (2017).

[16] 日本 IBM：Trusteer Pinpoint Detect（オンライン），入手先 ⟨https://www.ibm.com/jp-ja/marketplace/trusteer-pinpoint-detect⟩（参照 2018-12-05）．

[17] セキュアブレイン：PhishWall プレミアム・PhisWall クライアントレス（オンライン），入手先 ⟨https://www.securebrain.co.jp/products/phishwall/index.html⟩（参照 2018-12-05）．

[18] 全国銀行協会：インターネット・バンキングにおける預金等の不正な払戻しについて（オンライン），入手先 ⟨https://www.zenginkyo.or.jp/topic/detail/nid/6389/⟩（参照 2018-12-07）．

[19] 鈴木雅貴，中山靖司，古原和邦：インターネット・バンキングに対する Man-in-the Browser 攻撃への対策「取引認証」の安全性評価，金融研究，Vol.32, No.3, pp.51–76 (2013).

[20] 佐野宏明，田中英彦：インターネットバンキングの不正送金対策，第 77 回全国大会講演論文集，No.1, pp.443–444 (2015).

[21] 岡田周平，森　滋男，後藤厚宏：不正送金対策向け金融サイバーキルチェーン，コンピュータセキュリティシンポジウム 2016 論文集，Vol.2016, No.2, pp.1012–1018 (2016).

[22] Kiwia, D., Dehghantanha, A., Choo, K.-K.R. and Slaughter, J.: A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence, *Journal of Computational Science*, Vol.27, pp.394–409 (2018).

[23] Continella, A., Carminati, M., Polino, M., Lanzi, A., Zanero, S. and Maggi, F.: Prometheus: Analyzing WebInject-based information stealers, *Journal of Computer Security*, Vol.25, No.2, pp.117–137 (2017).

高田 一樹　（学生会員）

2003 年日本大学工学部情報工学科卒業．2005 年同大学大学院博士前期課程修了．2014 年株式会社セキュアブレインに入社．主に不正サイトの検知・分析，マルウェアの静的・動的解析，不正送金対策システムの研究開発に従事．2017 年横浜国立大学大学院環境情報学府入学．電子情報通信学会会員．

吉岡 克成　（正会員）

2005 年 3 月横浜国立大学大学院環境情報学府情報メディア環境学専攻博士課程後期修了．博士（工学）．同年 4 月独立行政法人情報通信研究機構で研究員として勤務．2007 年 12 月横浜国立大学学際プロジェクト研究センター特任教員（助教）．2011 年 4 月横浜国立大学大学院環境情報研究院准教授．マルウェア解析やネットワーク攻撃観測・検知等のネットワークセキュリティの研究に従事．2009 年文部科学大臣表彰・科学技術賞（研究部門），2016 年産学官連携功労者表彰総務大臣賞，2017 年情報セキュリティ文化賞をそれぞれ受賞．

松本 勉

1986 年東京大学大学院工学系研究科電子工学専攻博士課程修了．工学博士．同年より横浜国立大学勤務．現在，同大学・環境情報研究院教授および先端科学高等研究院情報・物理セキュリティ研究ユニット主任研究者および産業技術総合研究所サイバーフィジカルセキュリティ研究センター長．CRYPTREC 暗号技術検討会座長，日本学術会議連携会員を兼任．情報・物理セキュリティの研究教育に 1981 年より従事．この間，日本銀行金融研究所客員研究員，独カールスルーエ大学客員教授，日本学術振興会学術システム研究センター専門研究員，国際暗号学会 IACR 理事等を歴任．暗号学国際会議 ASIACRYPT，暗号と情報セキュリティシンポジウム SCIS 等の創設に貢献．電子情報通信学会業績賞，第 5 回ドコモ・モバイル・サイエンス賞，第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞，等受賞．