情報処理学会論文誌 Vol.59 No.3 1050–1060 (Mar. 2018)

ホワイトリストを用いた自律進化型防御システムの開発

重本 倫宏[1,2,a)] 藤井 翔太[1] 来間 一郎[1] 鬼頭 哲郎[1] 仲小路 博史[1] 藤井 康広[1] 菊池 浩明[2]

受付日 2017年6月26日, 採録日 2017年12月8日

概要：標的型攻撃に利用される遠隔操作型マルウェアによる被害を防ぐため，ブラックリストやホワイトリストを用いた対策が存在する．ブラックリストを用いた対策は，マルウェアがアクセスする接続先をブラックリストで管理し，当該接続先への通信を遮断するが，近年のマルウェアは接続先を頻繁に変更させるため，その変更に追随することが難しいという課題がある．一方ホワイトリストを用いた対策は，安全と分かっているサイトのみ接続を許可するが，ホワイトリストに登録されていないサイトへの通信が遮断されるため，ユーザの利便性が低下する（業務へ悪影響を与える）という課題がある．本稿では，未知の接続先への接続が発生した際に，マルウェア等のプログラムでは突破が困難な認証を要求する，ホワイトリストを用いた自律進化型防御システムを提案する．本提案システムにより，業務への悪影響を抑えつつ，遠隔操作型マルウェアの通信を遮断することが可能となる．また，評価実験により，提案システムの有効性を評価する．

キーワード：マルウェア，ホワイトリスト，CAPTCHA

Development of Autonomous Evolution of Defense System Based on Whitelist

Tomohiro Shigemoto[1,2,a)] Shota Fujii[1] Ichiro Kurima[1] Tetsuro Kito[1]
Hirofumi Nakakoji[1] Yasuhiro Fujii[1] Hiroaki Kikuchi[2]

Received: June 26, 2017, Accepted: December 8, 2017

Abstract: In order to minimize the damage by the Remote Access Tool (RAT) malware used in targeted attacks, various countermeasures such as blacklist approach and whitelist approach have been developed. Blacklist approach manages the servers where the malwares tried to communicate, and block communications of the malwares. However recent malware changes the C&C servers frequently, it has difficulty in following the change of servers. Whitelist approach permits only the servers already known as safe. It blocks communications where is not on the whitelist, thus it has caused disruptive effects on business. In this paper, we propose and evaluate Autonomous Evolution of Defense System based on Whitelist. Proposed system requests additional authentication which a program such as a malware cannot pass through, when unknown communication occurs. This system can take countermeasures such as the RATs malware without disruption of business activities.

Keywords: malware, whitelist, CAPTCHA

1. はじめに

近年，民間企業や政府機関，制御システム等の重要インフラを狙ったサイバー攻撃が顕在化しており，個人，企業，国家それぞれの利益や安全性を損なうリスクが高まっている．特に APT（Advanced Persistent Threat）攻撃 [1] は，秘密裏に，そして執拗に長期間攻撃を続ける点で従来の脅威とは異なり，マルウェアの侵入を検知あるいは防止することは不可能になりつつある．このような巧妙化する攻撃に対し，組織間でインテリジェンス（脅威情報や IT

[1] 株式会社日立製作所
Hitachi Ltd., Yokohama, Kanagawa 244–0817, Japan
[2] 明治大学
Meiji University, Nakano, Tokyo 164–8525, Japan
[a)] tomohiro.shigemoto.jh@hitachi.com

機器の脆弱性情報およびそれらに関する分析や対処支援情報）を共有して攻撃に備える集団防御の概念が浸透してきた．集団防御を実現するべく，ICT-ISAC[*1]等の公益法人や FireEye [2]，Threat Connect[*2]等の民間企業がインテリジェンスの共有を進めている．しかし，インテリジェンス共有の仕組みは整いつつあるもののインテリジェンスの活用が進んでいないのが実態である．たとえば，2015 年 6 月に日本年金機構が標的型攻撃を受けて 125 万件もの個人情報が漏えいし [3]，これを端緒として短期間に同様のマルウェアによって東京商工会議所や早稲田大学等，計 44 もの組織の情報漏えい被害が発生した [4]．この標的型攻撃では EMDIVI [5] と呼ばれる遠隔操作型マルウェアが用いられていたが，このマルウェアの特性や対処方法等のインテリジェンスが適切に共有され，かつ対策に迅速に活用されていれば，これらの被害の発生は抑えられたと考えられる．

著者らはこのような状況に鑑み，マルウェアの動的解析結果の情報や，共有されたインテリジェンスを活用することでサイバー攻撃に対して集団防御を実現する自律進化型防御システム（AED：Autonomous Evolution of Defense）の研究を進めてきた [6], [7]．マルウェアの中には，自身がインターネットと通信可能か否かを判断するために，実行初期に正規のサーバに対して疎通確認（HTTP 通信）を行うものが存在する．このため，マルウェアを動的解析した結果得られたマルウェアの通信先を HTTP プロキシ（以下，プロキシ）等で遮断すると，業務へ悪影響（可用性の低下）を与える可能性がある．我々の研究グループが提案する AED は，このような不確実性の高い脅威情報を用いて対策を実現するシステムである．具体的には，マルウェアの動的解析や共有されたインテリジェンスから得られた不審サイト情報（ホスト名（FQDN）および IP アドレス）をグレイリストとして管理し，クライアントがその不審サイトへアクセスしようとした場合に，プロキシで追加認証を要求する．これにより，たとえ誤った情報による認証追加であったとしても人間による業務上必要なアクセスは許可しつつ，マルウェア等の機械によるアクセスを遮断することを可能とする．最近は DGA（Domain Generation Algorithm）と呼ばれるドメイン生成アルゴリズム [8] を用いて，次々と新たなドメインを生成するものもあり，すべての接続先をあらかじめ把握することは困難になってきている．

そこで，本稿では不審サイトの情報（グレイリスト）を用いずに遠隔操作型マルウェアの通信を遮断する，ホワイトリストを用いた自律進化型防御システム（以下，ホワイトリスト型 AED）を提案する．ホワイトリスト型 AED では，安全なサイト（ホスト名（FQDN）および IP アドレス）をホワイトリストとして管理しており，ホワイトリストに合致しない接続先への HTTP 通信が発生した際に追加認証を要求する．これにより，未知のサイトを利用した攻撃にも対応することが可能となる．

まず，2 章では関連研究について述べ，3 章でホワイトリスト型 AED を提案する．4 章で提案システムの実装について説明し，5 章で実環境を用いた評価実験および，プロキシログを用いた有効性評価を行う．そして最後に 6 章でまとめを述べる．

2. 関連研究

遠隔操作型マルウェアを用いた攻撃への対策として，インターネットへの出口に設置したプロキシのユーザ認証機能を有効化することが推奨されている [9]．しかし，近年の遠隔操作型マルウェアの中にはプロキシ認証を突破するものも存在 [10] し，プロキシ認証が万全とはいえない状況となってきている【問題 1】．

また，マルウェアに感染したクライアントによる外部サイトへの情報漏えいを防止する製品として，インターネットへアクセスする際に CAPTCHA（Completely Automated Public Turing test to tell Computers and Humans Apart）[*3]認証を要求する製品が存在する [11]．CAPTCHA は機械と人とを判別する逆チューリングテストであり，マルウェアのようなプログラム（機械）では CAPTCHA を突破することができないという特性を利用する．しかし，本製品は，外部サイトに接続する度に CAPTCHA 認証を行っており，日々の業務の妨げとなる【問題 2】．

マルウェアの動的解析結果等の不確実なインテリジェンス（グレイリスト）をもとに，プロキシ等の出口対策のブラックリストに活用する手法が畑田らより提案されている [12]．また，悪性な社外サイトへのアクセスを防ぎつつも，安全性の高いサイトへのアクセス時には CAPTCHA 認証を省略することで業務への影響を軽減する手法が角田らにより提案されている [13]．しかし，これらの方式はまだ世の中に知られていない未知のサイトをマルウェアが利用したときに対策できない【問題 3】．

提案方式の特徴は，業務への悪影響を抑えつつ，未知のサイトを利用した攻撃に対処できることである．提案手法と既存技術との比較を**表 1** にまとめる．

表 1 既存技術との比較
Table 1 Comparison with existing countermeasures.

	【問題 1】認証突破 MW 対応	【問題 2】CAPTCHA 頻度	【問題 3】未知サイト対応
提案手法	可	低	可
認証プロキシ[9]	不可	-	可
CAPTCHA[11]	可	高	可
畑田ら[12]	可	-	不可
角田ら[13]	可	低	不可

[*1] https://www.ict-isac.jp/
[*2] https://www.threatconnect.com/
[*3] http://www.captcha.net/

3. ホワイトリスト型 AED の提案

本章では，ホワイトリストに定められた接続先以外には追加認証を要求することにより，人間による意図的な通信は許可するとともに，認証結果を用いてホワイトリストの精度を高めていく，ホワイトリスト型 AED を提案する．

3.1 サイバー攻撃の流れ

遠隔操作型マルウェアを用いたサイバー攻撃の流れを図 1 に示す．

まず，攻撃者は標的としている組織に，遠隔操作型マルウェアを添付したメールを送付（図 1①）する．組織のユーザが誤って添付ファイルを実行すると，遠隔操作型マルウェアに感染（図 1②）してしまう．組織に侵入した遠隔操作型マルウェアは，攻撃者との HTTP 通信を確立するため，外部にいる攻撃者に接続（図 1③）する．攻撃者は遠隔操作型マルウェアとの HTTP 通信を確立し，感染した端末を遠隔操作（図 1④）して内部情報の収集（図 1⑤）を行い，最終的に情報を搾取（図 1⑥）する．

提案するホワイトリスト型 AED では，遠隔操作型マルウェアが攻撃者と接続を行う点（図 1③）に着目し，ホワイトリストに存在しない接続先に HTTP 通信が発生した際に，マルウェアには解決困難な認証手段（提案システムでは CAPTCHA を用いるが，他の手段でもかまわない）を要求することで，遠隔操作型マルウェアによる HTTP 通信を遮断する．これにより，たとえ遠隔操作型マルウェアの組織侵入を許したとしても，マルウェアと攻撃者の通信を遮断し，情報漏えい等の事故を防止することが可能となる．

3.2 提案システムの概要

提案するシステムの概要を図 2 に示す．

提案するホワイトリスト型 AED は，認証プロキシ（認証機能付きプロキシ）と連携し，遠隔操作型マルウェアの通信を遮断する．ホワイトリスト型 AED が具備する 3 つの機能を以下に示す．なお，これらの機能の詳細については，3.3 節で述べる．

(1) 追加認証判定
接続先をホワイトリストや過去の追加認証判定結果と比較し，追加認証を要求するか否かの判定を行う機能

(2) 追加認証
ユーザに対する追加認証を生成し，追加認証に対する応答を受け取る機能

(3) ホワイトリスト更新
ユーザの追加認証結果を集計し，ホワイトリストの更新を行う機能

ホワイトリスト型 AED は，ユーザからの接続要求を受け取ると，接続先をホワイトリストや当該ユーザの過去の追加認証判定結果と比較し，追加認証を行うか否かの判定を行う．追加認証が必要と判定された場合は，追加認証（CAPTCHA）を要求する．ユーザが CAPTCHA を解釈し，正しく入力を行えば，当該接続は人による接続（遠隔操作型マルウェアによる C&C サーバへの通信ではない）と判断し，インターネットへの接続を許可する．

さらに，ある一定数のユーザが追加認証に成功している接続先は業務でよく利用される接続先と見なし，ホワイトリストに追加する．

以上のように，ホワイトリストと CAPTCHA を用いた接続制御により，遠隔操作型マルウェアの通信を遮断し，さらに，ホワイトリストの更新により，業務へ与える影響を抑制する．

3.3 提案システムの詳細

提案システムを構成する 3 つの機能の詳細を説明する．

(1) 追加認証判定

追加認証判定機能の処理フローを図 3 に示す．

追加認証判定機能では，プロキシサーバに届いたユーザからのリクエスト情報を受信し，接続先のドメインがホワイトリストに登録されているか否かを判断する．接続先

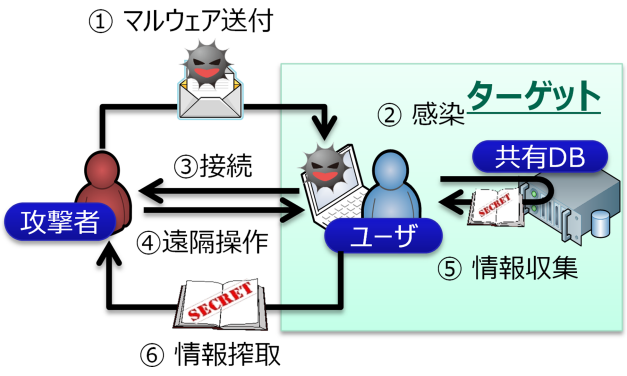

図 1 サイバー攻撃の流れ
Fig. 1 Overview of cyber attack.

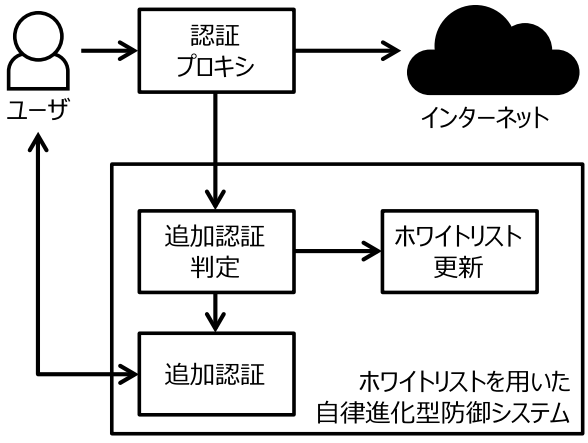

図 2 ホワイトリスト型 AED
Fig. 2 Overview of the AED based on whitelist.

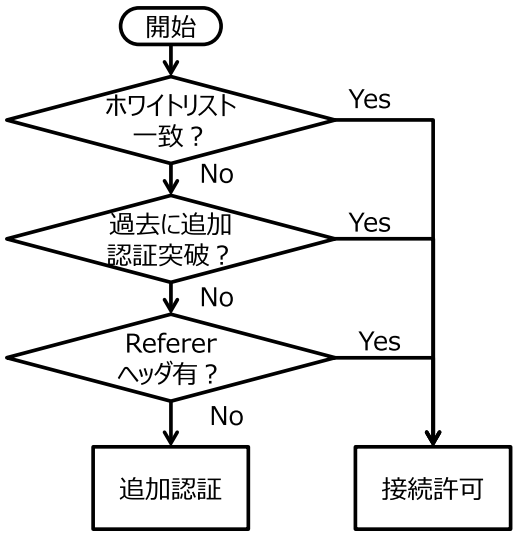

図 3 追加認証判定フロー
Fig. 3 Determination flow of additional authentication.

図 4 表示不具合の例（左：適用前[*4]，右：適用後）
Fig. 4 Example of problem (Left: before, Right: after).

のドメインがホワイトリストに登録されている場合には，ユーザの接続を許可し，登録されていない場合には，当該ユーザが，過去に当該接続先に接続を実施したか否かを判断する．当該ユーザが，過去に当該接続先に接続を実施していた場合には，ユーザの接続を許可し，接続を実施していない場合には，追加認証機能へリクエスト情報を送信する．

なお，HTML ファイルが外部サーバに格納された CSS ファイル等を参照していた場合にレイアウトが崩れる等の問題（**図 4** 左）が発生しないようにするため，ユーザからのリクエスト情報に Referer ヘッダが含まれている場合は接続を許可することとした．

また追加認証判定機能では，過去の接続状況を管理するため，以下の情報をアクセスログとして記録する．

- アクセス日時
- ユーザ識別用 ID（認証プロキシのユーザ名）
- アクセス元 IP アドレス
- アクセス先 URL
- Referer ヘッダの情報

[*4] CSS ファイルが読み込めず，左側のメニューや背景が表示されない不具合が発生している．

図 5 追加認証フォーム
Fig. 5 Screen capture of CAPTCHA.

(2) 追加認証

追加認証機能では，CAPTCHA 認証に必要な歪み画像および認証フォームの生成を行う．また，CAPTCHA に対するユーザ入力の正当性を判定する．追加認証機能が生成する認証フォームの例を**図 5** に示す．追加認証フォームには，「イメージ取得」ボタンも表示する．本ボタンを押下すると，ユーザが接続しようとしているサイトのスクリーンショットを取得し，ユーザに表示する．これは，ユーザの接続可否判断を補助するための措置である．

(3) ホワイトリスト更新

ホワイトリスト更新機能は，事前に定めたある一定以上のユーザが CAPTCHA を突破した場合には業務で利用する接続先と見なし，当該接続先をホワイトリストに登録する．

4. 実装

本章では，ホワイトリスト型 AED の実装について述べる．ホワイトリスト型 AED の各機能の構成を**図 6** に，これらの実装に用いたソフトウェアを**表 2** に示す．

なお，プロキシと Java の通信には ICAP（Internet Content Adaptation Protocol）[*5] を用いた．

5. 評価実験

本章では，開発したホワイトリスト型 AED の評価結果について述べる．

[*5] https://tools.ietf.org/html/rfc3507

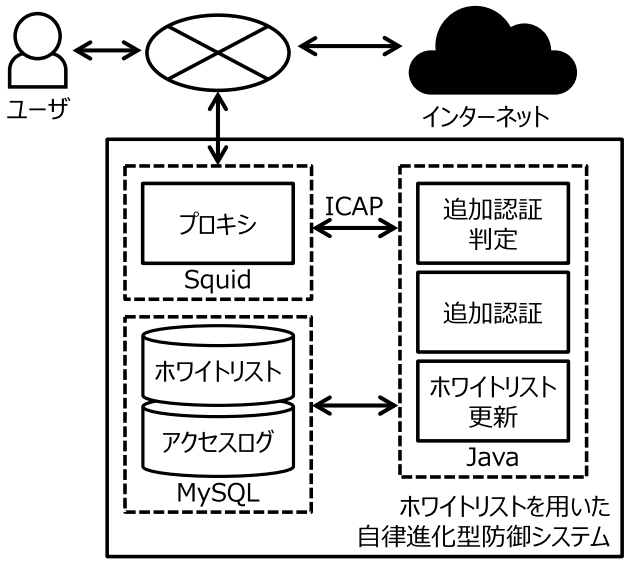

図 6 提案システムの実装
Fig. 6 Implementation of the proposed system.

表 2 実装に用いたソフトウェア
Table 2 Software used in the implementation.

機能	実装に用いたソフトウェア
追加認証判定機能，ホワイトリスト更新機能	Java 1.8.0
追加認証機能	Java Servlet 3.0
データベース（ホワイトリスト，アクセスログ）	MySQL 14.14
プロキシ	Squid 3.3.8

5.1 評価目的

ホワイトリスト型 AED は，業務への悪影響を抑えつつ，遠隔操作型マルウェアの通信を遮断するシステムである．遠隔操作型マルウェアの通信遮断精度と，業務への影響について，以下の観点で評価する．

(1) 遠隔操作型マルウェアの遮断精度について

開発したプロトタイプを用いた評価実験を行い，遠隔操作型マルウェアの通信遮断精度を評価する．

(2) 追加認証の要求率について

開発したプロトタイプを用いた評価実験を行い，業務時の追加認証要求率（総接続数に対する追加認証要求数の割合）を評価する．

(3) 業務への影響に関するアンケートについて

被験者へのアンケート調査により業務への影響度を評価する．

(4) ユーザ規模について

ホワイトリスト型 AED は利用するユーザが多いほど，業務への影響が抑制される．ホワイトリスト型 AED を利用するユーザ数を n とし，n と追加認証要求率の関係を評価する．

(5) ホワイトリスト更新の閾値について

ホワイトリスト型 AED はホワイトリスト更新の閾値が少ないほど，業務への影響が抑制される．ホワイトリストへ移行させるユーザ数を k とし，k と追加認証要求率の関係を評価する．

表 3 評価用遠隔操作型マルウェアの例
Table 3 Example of evaluation RAT malware.

種類	ハッシュ値（MD5）
Emdivi	e5653a4bca1239b095509438a3040244
PlugX	5a22e5aee4da2fe363b77f1351265a00
ChChes	8a93859e5f7079d6746832a3a22ff65c

5.2 評価方法

(1) 遠隔操作型マルウェアの遮断精度について

世の中に存在する遠隔操作型マルウェア（50 検体）を入手し，開発したプロトタイプを用いて，当該遠隔操作型マルウェアの通信を遮断できるか評価する．なお，評価に用いた遠隔操作型マルウェアの例を**表 3** に示す．

(2) 追加認証の要求率について

提案システムのプロトタイプを用いて業務時の追加認証要求率を評価する．具体的には，50 人のユーザに提案システムの利用を依頼し，初期ホワイトリストを空にした状態で実験を開始した．なお，標的型攻撃メール訓練の開封率が 10%である [14] ことから，組織内にはセキュリティ意識の低いユーザが 10%存在すると考えられる．本実験でもセキュリティ意識の低いユーザが 10%存在する（実験参加者の 10%は CAPTCHA が表示された際に内容を確認せずに入力してしまう）との仮説をたて，実験参加者の 10%以上のユーザが CAPTCHA 認証に成功した際にホワイトリストに追加することとした（$k = 5$）．

実験期間中は，ユーザ自身が普段利用するブラウザのプロキシ設定を変更し，WEB アクセスに際してホワイトリスト型 AED を経由するように設定する．なお，2016 年 2 月 8 日～2016 年 2 月 24 日まで実験を行った．

(3) 業務への影響に関するアンケートについて

「(2) 業務への悪影響について」の被験者に対し，実験終了後にアンケートを実施する．なお，アンケートはプライバシを考慮し，無記名で回答してもらう．

(4) ユーザ規模について

ホワイトリスト型 AED を利用するユーザ数（$n = 10$, 50, 100, 500, 1,000）について，追加認証の要求率を評価する．評価には，ある組織のプロキシアクセスログ（15 日分）を用い，ホワイトリスト型 AED を活用した場合の追加認証の要求率を机上検討する．具体的には，15 日分のプロキシアクセスログの中から n ユーザ分のアクセスログを抽出し，アクセスごとに図 3 に示した処理フローに従い，追加認証を要求するか否かを判定する．なお，追加認証を要求すると判定された際には，当該ユーザが追加認証を突破するものと仮定し，追加認証を突破したユーザ数が 5 ユー

表 4 遮断精度評価結果
Table 4 Result of blocking communications.

	遮断検体数	遮断精度
提案手法	50	100%
認証プロキシ[9]	41	82%

表 5 評価結果
Table 5 Result of evaluation.

項目	数	割合
追加認証有り	12,115	1.93%
- 回答有り	1,620	0.26%
- 回答無し	10,495	1.67%
追加認証無し	616,718	98.07%
- 追加認証成功済接続先への接続	122,467	19.48%
- Referer ヘッダがついた接続	473,677	75.33%
- ホワイトリストへの接続	20,574	3.27%
計	628,833	100.00%

ザ（$k = 5$）になった接続先はホワイトリストに追加する．これらの処理を行い，n ユーザ分の総接続回数に対する追加認証要求数を追加認証要求率として評価する．なお，評価は選択するユーザをランダムに変化させながら 10 回行い，その平均追加認証要求率を用いた．

(5) ホワイトリスト更新の閾値について

ホワイトリストへ移行させるユーザ数の閾値（$k = 1, 5, 10, 25, 50$）について，追加認証の要求率を評価する．評価には，ある組織のプロキシアクセスログ（15 日分）を用い，ホワイトリスト型 AED を活用した場合の追加認証の要求率を机上検討する．具体的には，15 日分のプロキシアクセスログの中から 100 ユーザ分（$n = 100$）のアクセスログを抽出し，アクセスごとに図 3 に示した処理フローに従い，追加認証を要求するか否かを判定する．なお，追加認証を要求すると判定された際には，当該ユーザが追加認証を突破するものと仮定し，追加認証を突破したユーザ数が k になった接続先はホワイトリストに追加する．これらの処理を行い，100 ユーザ分の総接続回数に対する追加認証要求数を追加認証要求率として評価する．なお，評価は選択するユーザをランダムに変化させながら 10 回行い，その平均追加認証要求率を用いた．

5.3 評価結果

(1) 遠隔操作型マルウェアの遮断精度について

評価用マルウェア（50 検体）に対する，遮断精度を**表 4** に示す．なお，認証プロキシを利用した手法 [9] との比較もあわせて示す．

表 4 より，提案手法は評価に用いた遠隔操作型マルウェアすべてを遮断することが確認できた．

(2) 追加認証の要求率について

実験期間中の総接続数と，追加認証有無の数を**表 5** に，ホワイトリスト数の推移を**図 7** に示す．なお，ノイズを除去するため，実験期間を通じて定常的にホワイトリスト型 AED の利用が確認された 24 ユーザ（7 日以上利用していたユーザ）を評価の対象とした（$n = 24$）．また，実験期間中に，検索エンジン（www.google.co.jp）や，総合情報サイト（itpro.nikkeibp.co.jp）等がホワイトリストに登録された．

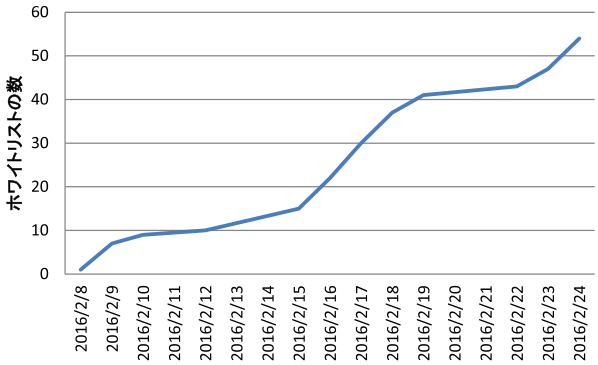

図 7 ホワイトリスト数の推移
Fig. 7 Transitions of the size of whitelist.

表 5 より，追加認証要求率は 1.93%であることが分かる．なお，実験期間中には遠隔操作型マルウェアによる被害が確認できなかった．これより，1.93%は正常な通信に対して誤って追加認証を要求，すなわちフォールスポジティブが生じたこととなる．また，Referer ヘッダがついた接続に追加認証を発生させないようにする処理は，追加認証の発生頻度削減に大きく貢献していることが確認できた．

また，追加認証の要求数は 12,115 回だったが，追加認証に対する回答は 1,620 回（1 ユーザあたり 1 日平均 3.97 回追加認証へ回答）しか観測されなかった．追加認証に対する回答がなかったサイトには，CRL や OCSP といった電子証明書関連情報を提供するサイトやソフトウェアの更新確認用サイト等が含まれていた．これらのサイトはブラウザや OS がバックグランドでアクセスするサイトのため，アクセスに際して発生した追加認証画面はユーザに提示されずタイムアウトしてしまう．このような接続先に関しては，あらかじめホワイトリストに登録することにより，追加認証の要求を抑制できると考える．

(3) 業務への影響に関するアンケートについて

被験者へのアンケート結果を**表 6** に示す．アンケートへの回答は 19 人から得られた．

追加認証の頻度がユーザの利便性に影響を与えるとの仮説をたて，当該仮説を検証するため Fisher の正確確率検定を用いて統計的に有意な差があるかどうかを分析した．検定結果を**表 7** に示す．

利便性に影響しないと考えるユーザ数（10 人）は，不便で影響ありとするユーザ数（9 人）を上回ったが，Fisher の正確確率検定の結果，追加認証の頻度とユーザの利便性の関係に有意な差が認められなかった．

また，アンケート結果より，約半数のユーザが不便と感

表 6 アンケート結果
Table 6 Result of questionnaire.

質問	選択肢	人数
追加認証はどれくらいの頻度で発生しましたか？	発生しなかった	0
	日に 1 回程度	3
	日に数回程度	13
	日に 10 回以上	3
追加認証の頻度についてどう感じましたか？	多くて不便	9
	この程度なら問題ない	10
	もっと多くても問題ない	0
期間中，追加認証の頻度は変化しましたか？	増えた	0
	変わらなかった	9
	減った	10

表 7 Fisher の正確確率検定
Table 7 Result of Fisher's exact test.

	この程度なら問題ない	多くて不便	p 値
追加認証が日に 1 回程度	3	0	
追加認証が日に数回	6	7	0.3731
追加認証が日に 10 回以上	1	2	
計	10	9	-

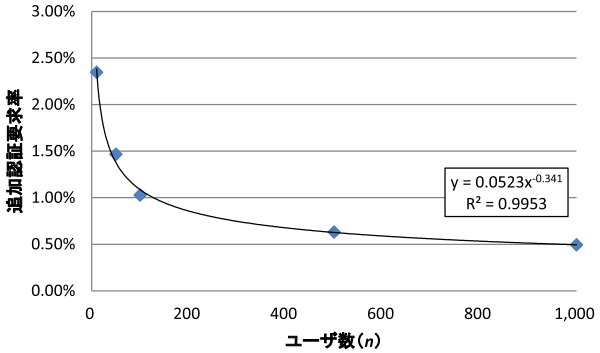

図 8 ユーザ数と追加認証要求率
Fig. 8 Requesting rate with regard to the size of n.

じていることが分かった．これについては，ホワイトリスト型 AED を利用するユーザ数を増やす，あるいは初期ホワイトリストを活用することで改善できると考える．実験期間中に追加認証の頻度が減ったと感じたユーザが存在したが，表 5 の結果より，これは，ホワイトリストが更新されたことによる効果ではなく，1 度認証に成功したドメインに対して認証を出さないようにする機能の効果だと考えられる．

(4) ユーザ規模について

ホワイトリスト更新の閾値を固定（$k = 5$）した状態で，ホワイトリスト型 AED を利用するユーザ数 n（n = 10, 50, 100, 500, 1,000）を変化させた際の追加認証要求率を**図 8** に示す．

図 8 より，ユーザ数が少ない範囲（n <= 200）では急速に追加認証要求率が減少するが，ユーザ数が多くなるに従い追加認証要求率の減少速度が低下することが分かる．

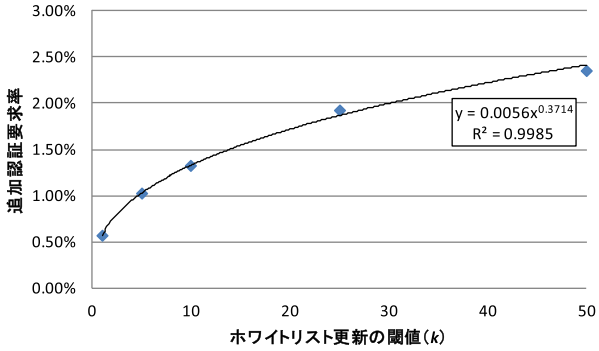

図 9 ホワイトリスト更新の閾値と追加認証要求率
Fig. 9 Requesting rate with regard to the size of k.

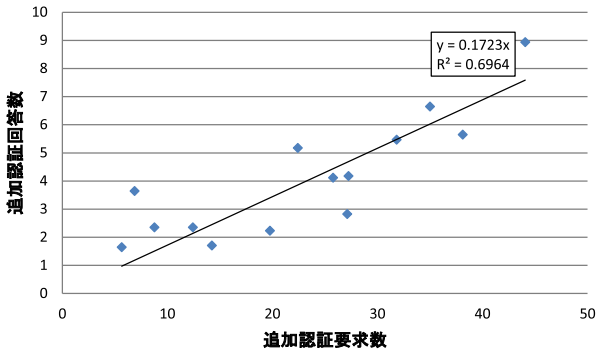

図 10 追加認証要求数と追加認証回答数
Fig. 10 Answering count vs requesting count.

(5) ホワイトリスト更新の閾値について

ホワイトリスト型 AED を利用するユーザ数を固定（n = 100）した状態で，ホワイトリストへ移行させるユーザ数の閾値 k（k = 1, 5, 10, 25, 50）を変化させた際の追加認証要求率を**図 9** に示す．

図 9 より，ホワイトリスト更新の閾値が大きくなるに従い，追加認証要求率の増加速度が低下することが分かる．また，k が 5 から 1 へ変化すると，追加認証要求率は約半分になることが確認できた．

5.4 考察

(1) 業務に影響を与えないユーザ規模について

プロトタイプを用いた評価実験結果から算出した，ユーザあたりの追加認証要求数（1 日あたり）と追加認証回答数（1 日あたり）の関係を**図 10** に示す．なお，ノイズを除去するため追加認証要求数の上位 5 ユーザと下位 5 ユーザのデータは除いてある．図 10 より，追加認証要求数に対する追加認証回答数はユーザごとにばらつきがあるが，ほぼ線形の関係にあることが分かる．

また，プロキシログを用いた机上検討結果から算出した，ユーザ規模とユーザあたりの追加認証要求数（1 日あたり）の関係を**図 11** に示す．図 11 より，ユーザ規模の増加にともない追加認証要求数は減少することが分かる．

さらに，アンケート結果（表 7）より，追加認証頻度が

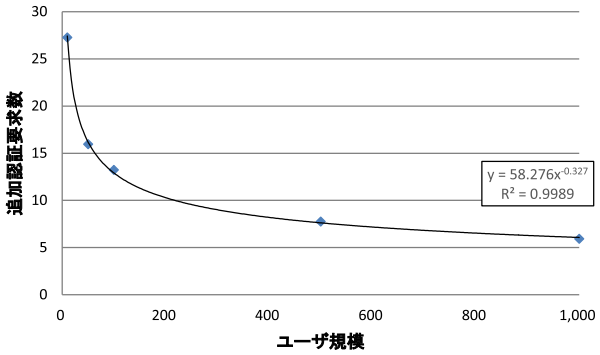

図 11 ユーザ数と追加認証要求数
Fig. 11 Requesting count with regard to the size of n.

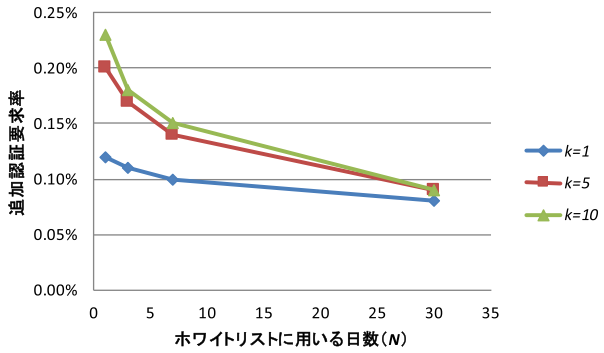

図 12 初期ホワイトリストと追加認証要求率
Fig. 12 Requesting rate with regard to the size of whitelist.

1 日に 1 回程度であれば不便を感じるユーザは存在しないことが分かる．図 10 の近似式より，1 日に 1 回程度の追加認証回答が発生するのは追加認証要求数が 5.8 回のときであり，図 11 より，1 日に 5.8 回の追加認証要求が発生するのはユーザ規模が 1,000 人程度であることが確認できる．以上より，ユーザ規模が 1,000 人程度になると，1 日の平均追加認証頻度が 1 回程度に抑えられ，業務に影響を与えることなく，遠隔操作型マルウェアの通信を遮断できるようになるといえる．

(2) 初期ホワイトリストの有効性について

評価実験により，電子証明書関連情報を提供するサイトやソフトウェアの更新確認用サイトはホワイトリストに移行されないことが分かった．このような接続先に関しては，あらかじめホワイトリストに登録することにより，追加認証の要求を抑制できると考えられる．ここでは過去 N 日（$N = 1, 3, 7, 30$）にユーザが接続した実績のある接続先を，初期ホワイトリストと定め，初期ホワイトリストを与えることにより，どの程度追加認証の頻度が削減されるかを考察する．具体的には，ホワイトリストに用いる日数 N を変化させながら初期ホワイトリストを生成し，5,000 人規模（$n = 5{,}000$）の組織のプロキシアクセスログ（30 日分）を用い，アクセスごとに図 3 に示した処理フローに従い，追加認証を要求するか否かを判定する．なお，追加認証を要求すると判定された際には，当該ユーザが追加認証を突破するものと仮定し，追加認証を突破したユーザ数が k になった接続先はホワイトリストに追加する．これらの処理を行い，総接続回数に対する追加認証要求数を追加認証要求率として評価する．ホワイトリスト更新の閾値 k（$k = 1, 5, 10$）とホワイトリストに用いる日数 N 日（$N = 1, 3, 7, 30$）を変化させた際の追加認証要求率を**図 12** に示す．

図 12 より，ホワイトリストに用いる期間が長いほど，追加認証要求率が低くなることが分かる．

なお，ここでは，過去当該組織がアクセスした接続先を初期ホワイトリストに加えたが，たとえば，遠隔操作型マルウェアがすでに組織に侵入していた場合には，遠隔操作型マルウェアの接続先が誤ってホワイトリストに追加されてしまう可能性がある．これに関しては，初期ホワイトリストに追加する際に，VirusTotal [*6]や，Site Safety Center [*7]等のレピュテーションサイトの情報と比較し，安全と判明しているサイトのみを登録することで解決できると考える．

(3) Referer ヘッダの有無について

提案システムでは，HTML ファイルが外部サーバに格納された CSS ファイル等を参照していた場合にも，正しく表示させるため，Referer 付きの通信に対する認証を省略することとした．この結果，ほとんどの場合ユーザは問題なく Web 利用可能であることが判明した．ただし，https で取得されたページから http でリソースを取得する場合等にはスキームが変化するため Referer が付かず，通信が遮断されるという問題があることが明らかになった．この問題については，引き続き対策を検討していく．

(4) 正規サイトを活用した遠隔操作について

遠隔操作型マルウェアの中には，Dropbox [*8]のような正規サイトを悪用して攻撃を行うものも存在する [15]．正規サイトがすでにホワイトリストに追加されている場合，ドメインレベルのホワイトリスト型 AED では対処することができない．このような問題に対応するためには，URL レベルでホワイトリストを作成する必要がある．しかし，URL レベルでホワイトリストを作成した場合には，追加認証の頻度があがり，業務へ影響を与えてしまう恐れがある．この問題についても引き続き対策を検討していく．

(5) 提案システムの処理性能について

考察 (1) において，提案システムが実用に耐えうるユーザ規模が 1,000 人程度であることを示した．ここでは，提案システムが 1,000 人規模の処理に耐えられるか否かを確認するため，Apache Jmeter [*9]を用いた性能評価を実施する．評価に利用した環境を**表 8** に示す．なお，ホワイトリストの登録数は，1,000 ユーザのプロキシログを用いた机上検討の際にホワイトリストに移行したドメイン数より決

*6 https://www.virustotal.com/ja/
*7 https://global.sitesafety.trendmicro.com/?cc=jp
*8 https://www.dropbox.com/ja/
*9 http://jmeter.apache.org/

表 8 評価環境の性能
Table 8 Specification of evaluation environment.

項目	値
CPU	Intel Core i5-3470 3.2GHz
Memory	4GB
ホワイトリストの数	21,000

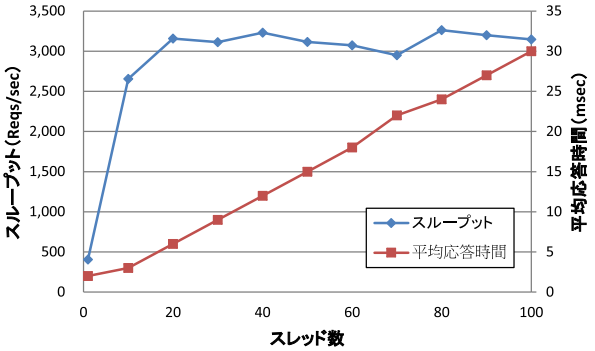

図 13 提案システムのスループットと平均応答時間
Fig. 13 Throughput and average response time of proposed system.

定した．

Jmeter の同時スレッド数を変化させながら計測した，スループットと平均応答時間を**図 13** に示す．なお，Jmeter のリクエストは，最も性能が要求される（追加認証が発生しない）パターンを用いた．

図 13 より，提案システムの処理性能は秒間 3,000 リクエスト程度であることが分かった．また，図 13 の平均応答時間が単調に増加していることより，処理性能の限界を超えたリクエストの処理待ちが発生し，応答時間の増大につながったと考えられる．なお，評価実験を通じて応答エラーは発生しなかった．1,000 ユーザのリクエストは，最大 748 リクエスト/秒（平均 22.9 リクエスト/秒）であったことから，処理性能の観点からは，提案システムによって 1,000 人規模のユーザを処理できることが確認できた．

(6) 提案システムの限界について

利便性とリスクのバランスを考慮し，提案システムでは Referer ヘッダが付いた通信の追加認証を省略する方針とした．これにより，Referer ヘッダを用いてランディングサイトを経由し，マルウェアをダウンロードさせる Drive by download 攻撃には対応できない．

また，提案システムでは 1 度ホワイトリストに入ってしまった正常サイトが乗っ取られてしまった場合は遠隔操作型マルウェアと攻撃者との通信を許すこととなる．この問題を解決するためには，セキュリティベンダの情報を監視し，正規サイトがクラックされた際には当該正規サイトの情報をホワイトリストから削除する必要がある．これにより，当該サイトへの通信に対して追加認証が発生し，遠隔操作型マルウェアの通信が遮断できるようになると考える．

6. おわりに

本稿では，ホワイトリストに定められた接続先以外には追加認証を要求することによって，人間による意図的な通信は許可するとともに，その認証結果を用いてホワイトリストの精度を高めていく，ホワイトリスト型の AED を提案し，プロトタイプを開発した．また，評価実験により，遠隔操作型マルウェアの通信を遮断できることを，ユーザの規模が少ないうちは，業務に与える影響が高い（追加認証要求率 1.93%）が，ユーザ規模が 1,000 人程度になると実用に耐えうることを確認した．以上の結果より，ホワイトリスト型 AED を用いることで，業務への影響を抑制しつつ，遠隔操作型マルウェアの通信を遮断できることを明らかにした．

今後は，大規模環境での実証を通じて，精度向上を行う．

本稿中で使われているシステム・製品名は，各社の商標または登録商標です．

参考文献

[1] IPA：標的型攻撃/新しいタイプの攻撃の実態と対策，入手先 ⟨http://www.ipa.go.jp/files/000024542.pdf⟩（参照 2017-06）．
[2] FireEye: FireEye Threat Intelligence, available from ⟨https://www.fireeye.jp/content/dam/fireeye-www/regional/ja_JP/products/pdfs/ds-threat-intelligence.pdf⟩ (accessed 2017-06).
[3] ラック：「日本年金機構の情報漏えい事件から得られる教訓」公開のお知らせ，入手先 ⟨http://www.lac.co.jp/news/2015/06/09_news_01.html⟩（参照 2017-06）．
[4] JPCERT：標的型攻撃への対応—JPCERT/CC，入手先 ⟨http://www.jpcert.or.jp/present/2015/JNSAWG20150625-apt.pdf⟩（参照 2017-06）．
[5] シマンテック：Backdoor.Emdivi，入手先 ⟨https://www.symantec.com/security_response/writeup.jsp?docid=2014-101715-1341-99⟩（参照 2017-06）．
[6] 仲小路博史，藤井康広，磯部義明，重本倫宏，鬼頭哲郎，林 直樹，川口信隆，下間直樹，菊池浩明：人間行動を用いた自律進化型防御システムの提案，暗号と情報セキュリティシンポジウム 2016（SCIS2016），pp.1–8 (2016).
[7] Nakakoji, H., Fujii, Y., Isobe, Y., Shigemoto, T., Kito, T., Hayashi, N., Kawaguchi, N., Shimotsuma, N. and Kikuchi, H.: Proposal and Evaluation of Cyber Defense System Using Blacklist Refined Based on Authentication Results, *2016 19th International Conference on Network-Based Information Systems* (*NBiS*), Ostrava, pp.135–139 (2016).
[8] Plohmann, D., Yakdan, K., Klatt, M., Bader, J. and Gerhards-Padilla, E.: A Comprehensive Measurement Study of Domain Generating Malware, *25th USENIX Security Symposium* (*USENIX Security 16*), Austin, pp.263–278 (2016).
[9] IPA：「高度標的型攻撃」対策に向けたシステム設計ガイド，入手先 ⟨https://www.ipa.go.jp/files/000046236.pdf⟩（参照 2017-06）．
[10] IIJ：新型 PlugX の出現，入手先 ⟨https://sect.iij.ad.jp/d/2013/11/197093.html⟩（参照 2017-06）．
[11] Digital Arts Inc.：Web プロキシ機能，入手先 ⟨http://www.daj.jp/bs/i-filter/function/proxy/⟩（参照 2017-06）．

[12] 畑田充弘，稲積孝紀，有川 隼，田中恭久：サンドボックス解析結果に基づく URL ブラックリスト生成方式に関する事例調査，信学技報，Vol.114, No.117, pp.309–314 (2014).
[13] 角田 朋，大鳥朋哉，藤井康宏，谷口信彦，木城武康：グレーリストを用いたホワイトリスト/ブラックリストの自動生成によるマルウェア感染検知方法の検討，情報処理学会研究報告．SPT，Vol.2014, No.16, pp.1–7 (2014).
[14] ASAHI INTERACTIVE, Inc.：標的型攻撃メール：政府機関の開封率 10%—教育で 3%に減少，思わぬ課題も見つかる，入手先 ⟨https://japan.zdnet.com/article/35013306/⟩（参照 2017-06）.
[15] トレンドマイクロ：起動日時が設定された RAT「PlugX」，入手先 ⟨http://blog.trendmicro.co.jp/archives/9357⟩（参照 2017-06）.

重本 倫宏 （正会員）

2006 年大阪大学大学院基礎工学研究科システム創成専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．現在はネットワークセキュリティ技術に関する研究開発に従事．明治大学大学院先端数理科学研究科先端メディアサイエンス専攻博士後期課程在籍．

藤井 翔太

2016 年岡山大学大学院自然科学研究科電子情報システム工学専攻修士課程修了．同年（株）日立製作所システムイノベーションセンタ入所．以来，ネットワークセキュリティ技術に関する研究開発に従事．

来間 一郎 （正会員）

2013 年東京大学大学院情報理工学系研究科修了．同年（株）日立製作所横浜研究所（現，システムイノベーションセンタ）入所．現在は，情報セキュリティの研究開発に従事．

鬼頭 哲郎 （正会員）

2005 年東京大学大学院情報理工学系研究科電子情報学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）に入所．以来，ネットワークセキュリティ技術に関する研究開発に従事．

仲小路 博史 （正会員）

2001 年東京理科大学大学院理工学研究科情報科学専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．以来，サイバー攻撃対策技術の研究開発に従事．現在，HITACHI EUROPE LTD. Senior Researcher．博士（理学）．

藤井 康広

2001 年東京大学大学院理学系研究科博士課程修了（物理学）．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．以来，情報セキュリティ技術，著作権保護技術，電子透かしおよび符号理論の研究開発に従事．現在，システムイノベーションセンタセキュリティ研究部主任研究員．博士（理学）．

菊池 浩明 （正会員）

1988年明治大学工学部電子通信工学科卒業．1990年同大学大学院博士前期課程修了．1994年同博士（工学）．1990年（株）富士通研究所入社．1994年東海大学工学部電気工学科助手．1995年同専任講師．1999年同助教授，2000年同電子情報学部情報メディア学科助教授，2006年同情報理工学部情報メディア学科教授．2008年同情報通信学部通信ネットワーク工学科教授．1997年カーネギーメロン大学計算機科学学部客員研究員．2013年明治大学総合数理学部先端メディアサイエンス学科教授．WIDEプロジェクト暗号メールシステムFJPEMの開発，認証実用化実験協議会（ICAT），IPA独創情報技術育成事業等に従事．1990年日本ファジィ学会奨励賞，1993年情報処理学会奨励賞，1996年SCIS論文賞，2010年情報処理学会JIP Outstanding Paper Award．2013年IEEE AINA Best Paper Award．2014年情報セキュリティ文化賞．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM各会員．本会フェロー．