業務支援ツールおよび欺瞞機構の併用による内部犯アラートシステムの提案

著者	奥村 紗名, 天笠 智哉, 井坂 佑介, 佐々木 葵, 山本 匠, 吉村 礼子, 河内 清人, 大木 哲史, 西垣 正勝
雑誌名	情報処理学会研究報告,セキュリティ心理学とトラスト (SPT)
巻	2022-SPT-46
号	8
ページ	1-6
発行年	2022-02-28
出版者	情報処理学会
権利	ここに掲載した著作物の利用に関する注意 本著作物の著作権は情報処理学会に帰属します。本著作物は著作権者である情報処理学会の許可のもとに掲載するものです。ご利用に当たっては「著作権法」ならびに「情報処理学会倫理綱領」に従うことをお願いいたします。 Notice for the use of this material The copyright of this material is retained by the Information Processing Society of Japan (IPSJ). This material is published on this web site with the agreement of the author (s) and the IPSJ. Please be complied with Copyright Law of Japan and the Code of Ethics of the IPSJ if any users wish to reproduce, make derivative work, distribute or make available to the public any part or whole thereof. All Rights Reserved, Copyright (C) Information Processing Society of Japan. Comments are welcome. Mail to address editj@ipsj.or.jp, please.
URL	http://hdl.handle.net/10297/00028909

Vol.2022-SPT-46 No.8
2022/3/7

業務支援ツールおよび欺瞞機構の併用による内部犯アラートシステムの提案

奥村紗名[1]　天笠智哉[1]　井坂佑介[1]　佐々木葵[1]
山本匠[2]　吉村礼子[2]　河内清人[2]　大木哲史[1]　西垣正勝[1]

概要：不正の主犯格は組織の内部者であることが多く，内部不正への対策は必須だが，内部犯は正規の権限を有しているため本人認証では対策が十分にできない．そのためリスク値を評価し，高リスクのユーザを特定する必要がある．しかし，業務内容は多岐に渡るため「正規業務」を定義することは非現実的であり，かつ，同一ユーザが同一業務を行う場合でさえ時と場合に応じて作業は変動し得るため「アノマリ」を見極めることも難しい．すなわち，正確にリスク値を算出することは容易ではなく，結果として誤検知の多発を招く．それ故，内部犯検知システムの実現にあたっては，いかに誤検知を低減させるかが肝要となる．そこで本稿では，ユーザの振る舞いにおける「正常」と「不正」を確実に抽出するためのサブシステムを導入することによって，内部犯アラートシステムの精度改善を試みる．提案方式は，導入するサブシステム同士が補い合うように併用することによって，内部犯検知における誤アラートを効果的に低減可能である．

キーワード：内部犯検知，UEBA，ワークフロー管理，欺瞞機構

An insider threat alert system using workflow support tool and deception mechanism

SANA OKUMURA[1] TOMOYA AMAGASA[1] YUSUKE ISAKA[1] AOI SASAKI[1]
TAKUMI YAMAMOTO[2] AYAKO YOSHIMURA[2] KIYOTO KAWAUCHI[2]
TETSUSHI OHKI[1] MASAKATSU NISHIGAKI[1]

Keywords: Insider threat Detection, User and Entity Behavior Analytics, Workflow management, Deception

1. はじめに

近年の調査[1]によると不正の主犯格は組織の内部者であることが多く,内部不正への対策が必須であると言える．しかし，内部犯は正規の権限を有しているため，本人認証は機能しない．よって，ユーザの振る舞いからリスク値を評価し，高リスクのユーザを特定する必要がある．

現在のゼロトラスト環境下では，企業システムによって各ユーザのアクティビティが細かにトレースされているため，蓄積された各種ログ情報をリスク値の算出に活用できる[2]．しかし，業務内容は多岐に渡るため「正規業務」を定義することは非現実的であり，かつ，同一ユーザが同一業務を行う場合でさえ時と場合に応じて作業は変動し得るため「アノマリ」を見極めることも難しい．すなわち，正確にリスク値を算出することは容易ではなく，結果として誤検知の多発を招く．それ故，内部犯検知システムの実現にあたっては,いかに誤検知を低減させるかが肝要となる．

そこで本稿では，ユーザの振る舞いにおける「正常」と「不正」を精査するためのサブシステムを導入することによって，内部犯検知システムの精度改善を試みる．ユーザの「正常」な振る舞いの精査には社内業務支援ツールを利用する.アラートにつながったユーザの振る舞いの根拠が，上司・同僚からの指示・依頼に依るものであった場合，アラートを取り下げることができる．ユーザの「不正」な振る舞いの精査には欺瞞機構を利用する．正常なユーザであれば欺瞞ファイルに積極的に接触することはないため，欺瞞環境下でのユーザの振る舞いに応じて，アラートを取り下げることができる．リスク値が閾値を超えたユーザのみを欺瞞環境に送ることにより，情報資産の保護とアラートの精査を同時に達成する．提案方式は，社内業務支援ツールと欺瞞機構を，互いが補い合うように併用することによって，内部犯検知における誤アラートを効果的に低減可能である．

本稿では，企業システムにユーザ登録されているユーザを「登録ユーザ」と呼び，登録ユーザが使用している情報端末を「登録デバイス」と呼ぶ．登録ユーザが登録デバイスを用いて社内業務に従事するにあたり，悪意のない状態で作業を行う場合を「正規ユーザ」，悪意の下に業務を行う登録ユーザを「内部犯」と呼び分ける．ある登録ユーザのリスク値が閾値を超えた場合，当該ユーザが「擬陽性ユー

1 静岡大学
Shizuoka University

2 三菱電機株式会社
Mitsubishi Electric Corporation

ザ」であることを知らせるアラートが発報される．発報に呼応してセキュリティ担当者が出動し，擬陽性ユーザが正規ユーザであるか内部犯であるかの確認が行われる．

2. 内部不正対策に関する既存研究と課題

2.1 リスクベース認証

リスクベース認証は，ユーザの振る舞いからリスク値を評価し，そのリスク値に応じてユーザ認証の強度を変更する認証方式である[3]．内部犯は登録ユーザであるため，ユーザの認証情報（記憶情報，所持情報，生体情報）を確認するタイプのユーザ認証は内部犯対策となり得ない．このため，ユーザやデバイスの状況や振る舞いからリスク値を評価し，高リスクのユーザを検出するという方法によって内部犯を炙りだす必要がある[2]．すなわち，リスクベース認証は内部犯対策の一方式として機能する．

リスクベース認証におけるリスク値は，典型的には，「正規ユーザの通常のログインパターン」からの逸脱を数値化したものである．ログインパターンとしては，企業システムにログインする際の IP アドレス，利用端末，時間帯等が使われることが多い[4]．パターンの逸脱という観点からは，リスクベース認証はアノマリ検知型の IDS（Intrusion Detection System），IPS（Intrusion Prevention System）と類似性があるといえる．また，リスクベース認証の中には，シグネチャ型の方式（より正確には，ブラックリストを併用する方式）も存在する[5]．

リスクベース認証によって内部犯検知を達成するためには，「正規ユーザの通常の業務パターン」を定義した上で，そこからの逸脱を数値化する必要がある．しかし，ログインパターンと違い，業務内容は多岐に渡るため，すべての「正規業務」を網羅してパターンを定義することは非現実的である．また，同一ユーザが同一業務を行う場合でさえ，時と場合に応じて作業は変動し得るため，通常の業務パターンに対する「アノマリ」を見極めることも容易ではない．すなわち，シグネチャ型のリスクベース認証の場合も，アノマリ型のリスクベース認証の場合も，内部犯のリスク値の算出が困難であるという問題が残る．

2.2 ゼロトラスト

近年の感染症の拡大に伴い，多くの組織でリモートワークの活用が広がったことで，企業のセキュリティ対策は境界防御からゼロトラスト防御へと移行した．ゼロトラスト防御では，ユーザの ID・パスワードが攻撃者に窃取されることも想定する．認証情報の窃取に成功した攻撃者は，内部犯と同等の能力を有することになる．すなわち，内部犯対策はゼロトラスト防御の一要素である．

ゼロトラスト防御においては，以下の 4 点が重要とされている[6]．

ID 管理の強化：IDaaS（Identity as a Service）を導入し，企業システム内のユーザ情報を一元管理する．従来の ID・パスワードによるユーザ認証だけでなく，使用デバイスやアプリケーションのセキュリティ状態によってアクセス制御を行う．

デバイス管理の強化：EMM（Enterprise Mobility Management）を導入し，企業システムに接続する登録デバイスを一元管理する．EDR（Endpoint Detection and Response）を導入し，企業システムに接続する登録デバイスの動作状況を一元監視する．EMM は，MDM（Mobile Device Management)によるデバイス自体の管理と MAM (Mobile Application Management）によるデバイス内アプリの管理に大別される．EMM により，各デバイスのストレージを「企業領域」と「個人領域」を分割し，企業データを個人領域に持ち出すことを禁止することも可能である．EDR は，各デバイスの操作ログ，プロセスログ，通信ログ等を記録する．これらのログデータを用いてデバイスの状況や内容を常時監視し，異常あるいは不審な挙動を検知する．

ネットワークセキュリティ対策：SWG（Secure Web Gateway）を導入し，企業システムに接続する登録デバイスからの Web アクセスを一元管理する．CASB（Cloud Access Security Broker）を導入し，企業システムに接続する登録デバイスからのクラウドアクセスを一元管理する．SDP（Software Defined Perimeter）を導入し，企業システム内の情報資産や企業システムに接続する登録デバイスへのインバウンドアクセスを一元管理する．

セキュリティ運用の自動化：SIEM（Security Information and Event Management）を導入し，EDR，IDaaS，SDP 等の各種ログデータを一元管理し，企業システム内の情報資産や企業システムに接続する登録デバイスへの不正アクセスを検出する．SOAR（Security Orchestration, Automation and Response）を導入することにより，脅威インテリジェンス等を活用してセキュリティ運用を更に自動化することも可能である．

ゼロトラスト防御においては，ユーザやデバイスが企業システム内の情報資産へアクセスする度にユーザ認証が適用される．そして，上述の各種ツールが個々に，あるいは連携してユーザやデバイスの振る舞いを常に監視し続け，その挙動が前もって定められたリスク値を超えた時点でアラートが発報される[2]．この観点からは，ゼロトラスト防御とはリスクベース認証（2.2 節）を精緻化した仕組みであると捉えることができる．したがって，ゼロトラスト防御は内部犯にも一定の効果を発揮する．しかし，2.2 節で述べたように，正規の業務と不正な業務を明確に区別すること自体が難しい以上，単にログデータを増やすだけではリスク値の推測精度を高めるには限界がある．

2.3 社会技術的対策，社会科学的対策

Hunker らは，内部不正対策を技術的対策，社会技術的対策，社会科学的対策の 3 つに大別している[7]．技術的対策については，2.1 節，2.2 節で概説したため，本節では社会技術的対策および社会科学的対策について取り上げる．

社会技術的対策では，ポリシを用いて許される行動と許されない行動の境界を定義する．しかし，依然として内部犯の定義の困難性が課題として残る．内部犯とは「組織への情報資産にアクセスする権限を持っており，その権限を用いて情報資産を侵害した個人を指す[8]」が，この定義は非常に曖昧であり，明確なポリシの策定は容易なことではない．

社会科学的対策では，内部犯の心理的な側面や動機についても調査し，対策を行う．しかし，企業は風評被害等を恐れ，内部不正の発生を公表することは稀であるため，調査に資するデータの収集にハードルが存在する．この課題に対し，島らは，内部犯（情報漏洩）のシナリオを用意し，ロールベースのアンケート調査を行うことで内部不正に関する意識を収集する方法を採用している[9]．一方で，実データの入手困難性は，発生件数や傾向などを知ることさえ難しいという事実を突きつけており，実データに基づいて内部犯対策を分析，考察するという社会科学的対策のアプローチに課題を残している．

3. 提案

3.1 コンセプト

内部犯検知システムの実現にあたっては，いかに誤検知を低減させるかが肝要となる．この課題に対し，社内業務支援ツールと欺瞞機構を，ユーザの振る舞いにおける「正常」と「不正」を精査するためのサブシステムとして活用することによって，内部犯検知システムの精度改善を試みる．提案方式は，社内業務支援ツールと欺瞞機構を，互いが補い合うように併用することによって，内部犯検知における誤アラートを効果的に低減可能である（図 1）．

ある登録ユーザのリスク値が閾値を超え，アラートが発報された場合，まず，社内業務支援ツールに記録されている当該ユーザ(擬陽性ユーザ)のワークフローを確認する．アラートにつながった擬陽性ユーザの振る舞いの根拠が，上司・同僚からの指示・依頼に依るものであった場合は，アラートを取り下げることができる（ユーザの「正常」な振る舞いの精査）．

社内業務支援ツールによって救済されなかった擬陽性ユーザに対しては，欺瞞機構を起動し，「木を森に隠す」アプローチによって情報資産の保護を開始する．欺瞞機構の適用は，正規ユーザに利便性の低下を強いる．このため，ユーザの申告をもってアラートを取り下げるという運用を追加する．すなわち，アラートにつながった擬陽性ユーザの振る舞いの根拠を，ユーザ自らに説明させることによって，利便性低下に対する救済とアラートの精査（ユーザの「正常」な振る舞いの精査）を同時に達成する．

欺瞞環境下に置かれているにも関わらず，自己申告しない擬陽性ユーザは，自身の行動に後ろめたさを感じて申告を躊躇している内部犯か，何らかの理由で欺瞞環境下での業務遂行が必要な正規ユーザのいずれかである．後者は，正規業務の範疇の中に「欺瞞環境下での業務」が含まれていることを意味するため，欺瞞機構の詳細が当該ユーザに伝えられているはずである．すなわち，「自己申告をしない正規ユーザ」は，正規ファイルと欺瞞ファイルの識別が可能であると言える．正規ユーザであれば欺瞞ファイルに積極的に接触することはないため，欺瞞ファイルへのアクセスが確認された時点で内部犯の確証となる（ユーザの「不正」な振る舞いの精査）．

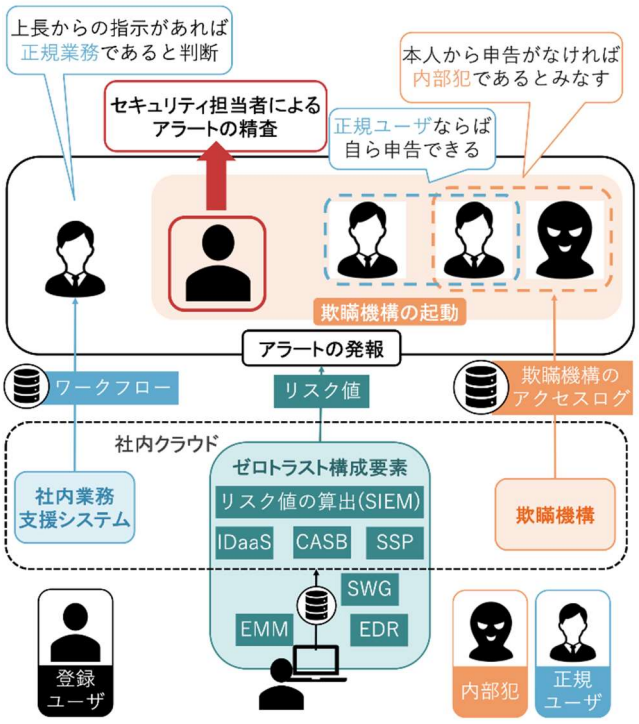

図 1 提案方式

3.2 社内業務支援システム

企業では，社内の DX（Digital Transformation）の一環で，ワークフローを管理する社内業務支援システムの運用が始まっている[10]．メール等の文面を自動的に分析し，社員のスケジュールを社内業務支援システムに自動的に反映させること等も可能である[11]．更には，スマートコントラクト[12]や RPA（Robotic Process Automation）[13]等を活用して，ある業務に続く次の業務を自動生成し，担当者を自動的にアサインすることも検討されている．今後は更に企業の DX が推進されていく中で，社員（登録ユーザ）の日々の業務は，属性情報（業務がアサインされた日時，業務を指示・

依頼した上司・同僚，業務完了期限，等）とともに，その内容が社内業務支援システムの中で管理されていくようになると考えられる．

そこで本稿では，社内業務支援システムによって管理される情報を，ユーザの「正常」な振る舞いを精査するために利用する．ある登録ユーザのリスク値が閾値を超え，アラートが発報された場合，社内業務支援ツールに記録されている当該ユーザ（擬陽性ユーザ）のワークフローを確認する．アラートにつながった擬陽性ユーザの振る舞いの根拠が，上司・同僚からの指示・依頼に依るものであった場合は，当該ユーザの行動は正規業務の中で発生した作業であると演繹できる．この結果，当該アラートを取り下げることが可能であり，ユーザの「正常」な振る舞いの精査が達成される．

ただし，社内業務支援システムのカバレッジには限界がある．まず，日本の構造的な問題として DX が立ち遅れており，現在の社内業務の DX 移行はまだまだ限定的である．また，オンライン管理に適さない（あるいは親和性の低い）業種・業務も存在する．仮に社内業務管理が完全にオンライン化されたとしても，オフラインチャネル（口頭や電話等）による業務指示・依頼の伝達は残ると予想される．更には，社員が自らの創意工夫の下に自発的に作業を行うことは奨励されるべきことであり，正規業務中に上司・同僚からの指示・依頼がない作業が発生することは，むしろ当然であると言える．

3.3 欺瞞機構

欺瞞機構とは，偽情報（データ，ファイル，サーバ，ネットワーク等）を配置し，攻撃者を欺くセキュリティ対策である．サイバー攻撃は巧妙化・多様化しており，企業システムへの侵入を完全に防ぐことは困難である．そのため，侵入されることを前提とした対策が必須であり，欺瞞機構はその一つとして用いられている．

Yuill らは，偽物のファイルを用いた攻撃検知手法を提案している[14]．攻撃者を誘引するために実物を模倣した囮ファイルを作成し，囮ファイルに対するアクセスが発生した際にアラートを発報する．角丸らは，「縦深防御」の概念の下に，効果的な欺瞞機構の構築方法を論じている[15]．欺瞞機構を用いて，攻撃者が得ようとする機密情報の価値よりも攻撃に要するコストを高く押し上げることで，攻撃者の動機を消失させる．これら欺瞞機構において肝要となるのが，偽情報の模倣精度である．本物と偽物が判別できてしまうと，攻撃者に欺瞞機構の迂回を許してしまい，安全性が低下する．本物と偽物が判別できないと，正規ユーザの困惑を招いてしまい，利便性が劣化する．この問題に対し，青池ら[16]は，正規ユーザのログアウト時のみ欺瞞機構を起動することによって，また，長谷川ら[17]は，正規ユーザ（GUI 操作者）のみが囮ファイルを視認できる「視覚型欺瞞化」を採用することによって，正規ユーザの利便性改善を模索している．しかし，本物と偽物の判別の難易の問題はトレードオフの関係にあるため，利便性と安全性を兼ね備える欺瞞機構の実現は一筋縄ではない．

そこで本稿では，利便性を敢えて低下させた形で欺瞞機構を運用することによって，欺瞞機構に対するユーザのリアクションを強制的に引き出し，これをユーザの「正常」あるいは「不正」な振る舞いを精査するために利用することを提案する．ある登録ユーザのリスク値が閾値を超え，アラートが発報された場合，当該ユーザ（擬陽性ユーザ）に対して欺瞞機構が起動する．提案方式の欺瞞機構は，正規ユーザの正規業務に支障をきたす程度に，その利便性が抑制されている．この不便利に耐えきれない正規ユーザは，企業システムを管理するセキュリティ担当者に，欺瞞環境に拘留された理由を伝えることによって，救済を申請することが許されている．

正規ユーザならば，躊躇なく，セキュリティ担当者に申し出て，「自分がどのような作業を行った結果，欺瞞環境に取り込まれてしまったのか」を説明することができる．一方，内部犯にとっては，それを説明することは，自身の悪事を自ら吐露することを意味するため，セキュリティ担当者に言うに言えない状況に陥る．よって，擬陽性ユーザから救済の申告があったこと自体が，当該ユーザが正規ユーザであることの証明になる．この結果，当該アラートを取り下げることが可能であり，ユーザの「正常」な振る舞いの精査と利便性低下に対する救済が同時に達成される．

ユーザのリスク値が閾値を超えた際に欺瞞機構が起動するため，擬陽性ユーザが欺瞞環境に取り込まれた理由が，当該ユーザのリスク値が閾値を超えた原因に直結する．当該ユーザのリスク値が閾値を超えた理由を見極めることは，セキュリティ担当者の重要な業務の一つである．従って，欺瞞環境に取り込まれた理由を擬陽性ユーザ自身に説明させるという運用は，この観点からも理に適っている．

欺瞞環境下に置かれているにも関わらず，自己申告しない擬陽性ユーザは，自身の行動に後ろめたさを感じて申告を躊躇している内部犯か，何らかの理由で欺瞞環境下での業務遂行が必要な正規ユーザのいずれかである．後者は，正規業務の範疇の中に「欺瞞環境下での業務」が含まれていることを意味するため，欺瞞機構の詳細が当該ユーザに伝えられているはずである．すなわち，「自己申告をしない正規ユーザ」は，正規ファイルと欺瞞ファイルの識別が可能であると言える．正規ユーザであれば欺瞞ファイルに積極的に接触することはないため，欺瞞ファイルへのアクセスが確認された時点で内部犯の確証となる．この結果，セキュリティ担当者による当該アラートの発生原因の究明を伴うことなく，ユーザの「不正」な振る舞いの精査が達成される．

欺瞞機構は「木を森に隠す」アプローチによる情報資産

の保護であるが，利便性を著しく低下させた欺瞞機構を採用する提案方式においては，縦深防御[15]のアプローチ（攻撃者が得ようとする機密情報の価値よりも攻撃に要するコストを高く押し上げることで，攻撃者の動機を消失させる）による情報資産の保護も達成しているといえる．前述の通り，利便性と安全性はトレードオフの関係にあるため，欺瞞機構の利便性を低下させるという提案方式の運用が，高い安全性を備える欺瞞機構の適用を可能としている．

3.4 社内業務支援システムと欺瞞機構の併用

提案方式のフローチャートを図 2 に示す．ある登録ユーザのリスク値が閾値を超え，アラートが発報された場合，提案方式はまず，社内業務支援ツールに記録されている当該ユーザ（擬陽性ユーザ）のワークフローを検査する．擬陽性ユーザの振る舞いの根拠が，上司・同僚からの指示・依頼に依るものであることが確認できたなら，アラートを取り下げ，それ以外の擬陽性ユーザのみに対して欺瞞機構を適用する．提案方式では，正規業務に支障をきたすほどに利便性を低下させた形で欺瞞機構を運用する（3.3 節）ため，欺瞞機構が適用される正規ユーザは可能な限り少数になるようにしたい．提案方式が，社内業務支援ツールによって救済されなかった擬陽性ユーザのみに対して欺瞞機構を適用するのは，この理由に依る．

アラート発報時にはセキュリティ担当者が出動し，当該ユーザ（擬陽性ユーザ）のリスク値が閾値を超えた原因の究明が行われることになる．誤アラートの抑制は，セキュリティ担当者の負荷低減に直結する非常に重要な要件である．社内業務支援システムにはカバレッジの限界がある（3.2 節）ため，社内業務支援ツールを用いたアラートの精査によって，すべての正規ユーザを救済することはできない．提案方式では，社内業務支援ツールを用いたアラートの精査の後段に，欺瞞機構を用いたアラートの精査を併用することによって，この問題に対処している．提案方式であれば，セキュリティ担当者が直接原因の究明を行うべき対象は，「欺瞞機構に捕らわれているのに，救済を求めない擬陽性ユーザ」のみとなる（図 1）．なお，擬陽性ユーザが内部犯であった場合，セキュリティ担当者が原因究明を終えるまでの間，内部犯は擬陽性ユーザとして企業システム内に潜在し続けることになるが，情報資産は欺瞞機構による保護下にあるので，許容し得る範囲内であると考えている．

4. まとめ

本稿ではユーザの振る舞いにおける「正常」と「不正」を確実に抽出するためのサブシステムを導入することによって，内部犯アラートシステムの精度を改善するシステムを提案した．サブシステムにはそれぞれ課題があるが，2 つのシステムを巧みに組み合わせることで課題が解決されることを確認した．今後の課題として，業務支援システムを用いた指示の抽出とユーザの振る舞いとの照合の精度の検証や，欺瞞機構でも検出できない内部犯の検知手法の検討が挙げられる．

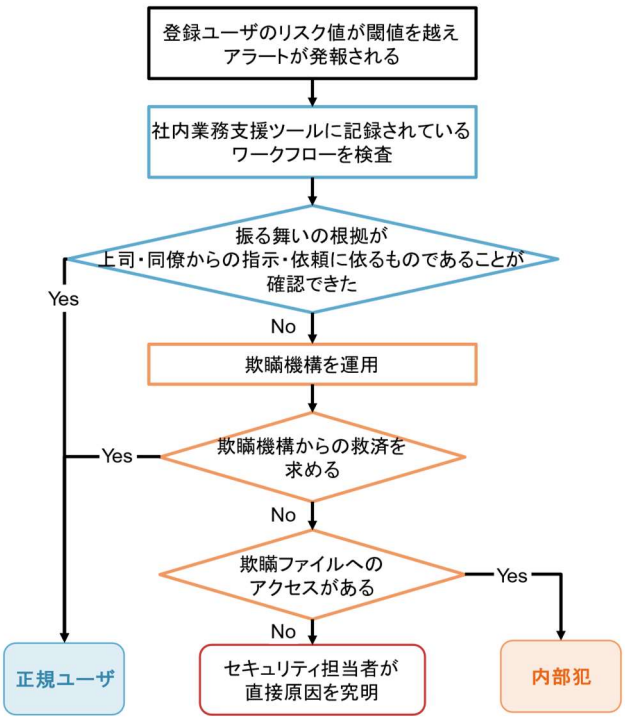

図 2 提案方式におけるアラート精査のフロー

参考文献

[1] PwC Japan グループ：経済犯罪実態調査 2020 ―日本分析版―，PwC （オンライン），入手先〈https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2020/assets/pdf/economic-crime-survey.pdf〉（参照 2022-2-2）．
[2]藤井翔太，来間一郎，磯部義明：エンドポイントログを用いた内部不正に係る挙動に着目した不正スコアリング手法の提案，マルチメディア,分散協調とモバイルシンポジウム 2019 論文集，pp.470-477（2019）．
[3] NEC：リスクベース認証，NEC（オンライン），入手先〈https://www.nec-solutioninnovators.co.jp/ss/insider/security-words/24.html〉（参照 2022-2-2）．
[4]瀬戸洋一：認証技術の種類と動向，電気設備学会誌，Vol.30，No.10，pp.809-812（2010）．
[5]Capy Inc.：apy Inc.、不審な IP アドレスを検知する『Capy リアルタイムブラックリスト』の提供を開始，Capy Inc.（オンライン），入手先〈https://corp.capy.me/ja/press_release/realtime_blacklist〉（参照 2022-2-2）．
[6]独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 4 期生 ゼロトラストプロジェクト：ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～，IPA（オンライン），入手先〈https://www.ipa.go.jp/files/000092243.pdf〉（参照 2022）-2-2）．
[7]Hunker, J., Probst, W.C.: Insiders and Insider Threats An Overview

of Definitions and Mitigation Techniques, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol.2, No.1, pp.4-27(2011).
[8]National Cybersecurity and Communications Integration Center: Combating the Insider Threat, National Cybersecurity and Communications Integration Center(online), available from 〈https://www.cisa.gov/sites/default/files/publications/Combating the Insider Threat_0.pdf〉 (accessed 2022)-2-2).
[9]島成佳：内部不正による情報セキュリティインシデントにおける内部者の意識と対策に関する分析と考察，コンピュータセキュリティシンポジウム 2012 論文集，Vol.2012，No.3，pp.539-546（2012）.
[10]角田忠信，山口純平，坂巻慶行ほか：信頼情報を基にした業務高信頼化方式，暗号と情報セキュリティシンポジウム 2022 1B1-2（2022）.
[11]Microsoft：メールから予定表にイベントを自動的に追加する，Microsoft（オンライン），入手先〈https://support.microsoft.com/ja-jp/office/メールから予定表にイベントを自動的に追加する-32e5cf0c-3e65-4870-9ff9-df3683d3fc97〉（参照 2022-2-2）.
[12] IBM：ブロックチェーンのスマート・コントラクトとは，IBM（オンライン），入手先〈https://www.ibm.com/jp-ja/topics/smart-contracts〉（参照 2022-2-2）.
[13]NEC：RPA を活用してワークフローシステムで業務効率化－EXPLANNER シリーズで業務の効率化：EXPLANNER，NEC（オンライン），入手先〈https://jpn.nec.com/soft/explanner/ai-iot/fl_rpa/index.html〉（参照 2022-2-2）.
[14] Yuill, J., Zappe, M., Denning, D., et al.: Honeyfiles: deceptive files for intrusion detection, Proceedings of the Annual IEEE SMC Information Assurance Workshop(online), DIO:10.1109/IAW.2004.1437806(2004).
[15]角丸貴洋，島成佳，渡部正文ほか：標的型攻撃対策に向けた欺瞞機構を用いた防御アーキテクチャ，電子情報通信学会技術研究報告，Vol.114，No.118，pp.69-74（2014）.
[16]青池優，神薗雅紀，衛藤将史ほか：欺瞞機構に伴う利便性低下を防止するためのおとりファイル非表示化，コンピュータセキュリティシンポジウム 2019 論文集，pp.691-696（2019）.
[17]長谷川翔，澤村遼，北川沢水ほか：欺瞞機構に伴う利便性低下を防止するためのおとりファイル非表示化，コンピュータセキュリティシンポジウム 2020 論文集，pp.567-572（2020）.