7E-02

組織間信頼度による匿名化処理を用いたインシデントチケット共有システムの開発

植木　優輝†　　重本　倫宏†　　川口　信隆†　　西嶋　克哉†
近藤　賢郎‡　　中村　修§
株式会社日立製作所　研究開発グループ†
慶應義塾　情報セキュリティインシデント対応チーム‡　慶応義塾大学　環境情報学部§

1. はじめに

近年，サイバー攻撃は攻撃者の技術力の誇示や愉快犯を目的としたものから，Advanced Persistent Threat (APT) 攻撃[1]を例とした，金銭や個人情報の奪取などを目的としたものへと変化してきている．このような巧妙化する攻撃に対して，自組織だけで防御をすることは困難である．そこで，日立製作所では，慶應大学と協力して，複数組織の SOC（Security Operation Center）を跨ったセキュリティオペレーション連携により，サイバー攻撃への集団防御を実現する分散 SOC アーキテクチャを提案している[2]．

本稿では，各組織がインシデント管理に用いるインシデントチケット（以下チケット）を，情報提供者と利用者間の信頼度を用いたアクセスコントロールを用いて共有するシステムを開発したので報告する．

2. 関連技術

本稿のように，複数組織における情報共有についての研究が行われている．S. N. Khajeddin ら[3]は，情報共有の課題とさまざまな信頼モデルについて述べている．しかし，情報共有プラットフォームの実装については述べておらず，本稿はこの点で異なる．

また，本稿のようにセキュリティインシデントに関する情報を複数組織で共有することは，既に行われている．例えば，公益法人である ISAC では，参加する各組織が共有するに値するインシデント情報を専用のポータルを用いて ISAC に共有し，これらの情報をまとめたものを定期的に発信している[4]．しかし，この手法では，個人情報等の機微情報や，社外秘情報等の機密情報が完全に排除された情報しか共有できない．また，情報共有に入力等の手間がかかるために，共有されるまでに時間がかかる．

3. 提案手法

サイバー攻撃者はほとんど同じ技術，戦術，手順を利用して，さまざまな企業やプラットフォームを攻撃することが多い[3]．そのため，インシデントの発生要因，検知・対処情報等を共有することで，潜在的脅威を特定することができる．また，これらの情報をインシデント発生時に迅速に共有することで，複数組織で連携してインシデント対処を行うことができる．迅速な情報共有を実現する一つの手段として，情報共有の自動化が挙げられる．しかし，情報には機微，機密情報が含まれているため，外部へ共有する前に自動化が困難な匿名化が必要である．

本稿では上記したインシデントに関する情報を各組織間の信頼度に応じて秘匿化し，信頼度が低ければ情報によっては匿名化を施して共有することで，情報共有の自動化を可能にするシステムを開発した．共有する情報の媒体は，組織がインシデント管理に用いるチケットを用いた. 図 1 にシステムの概要図を示す．

図 1 では，組織 A が持つチケットを，組織 B，組織 C へ共有する場合を表している．まず，組織 A のチケットが更新されると，チケット情報が組織 A の持つクライアント装置によって，3 段階のレベルに秘匿化される．秘匿化された情報群は中継装置に送られる．中継装置は情報を送信した組織 A と，組織 B，組織 C 間の信頼度を信頼度 DB から取得し，これに応じてどの秘匿レベルの情報を送信するか判別し，送信する．例えば，組織 A から組織 B への信頼度が低い場合は秘匿レベルが高い情報が送信され，組織 A から組織 C への信頼度が高い場合は秘匿レベルが低い情報が送信される．情報を共有された組織は，共有

Development of an incident ticket sharing system using anonymization processing based on inter-organizational trust score
† Yuki Ueki, Tomohiro Shigemoto, Nobutaka Kawaguchi, Katsuya Nishijima・Hitachi, Ltd. Research and development group
‡ Takao Kondo・Keio University Information security incident response team
§ Osamu Nakamura・Keio University Faculty of Environment and Information Studies

された情報を閲覧し，自組織のインテリジェンスリソース内に関連する情報があった場合これを返す．図1の場合，組織Cが関連するインテリジェンスを持っていたため，関連する情報を自組織内のクライアント装置で秘匿化し，中継装置を介して組織Aにフィードバックする．これにより，組織Aがインシデント対応中のチケットを送信していた場合，フィードバックされたインテリジェンスを用いて，迅速な対処を行うことが可能になる．

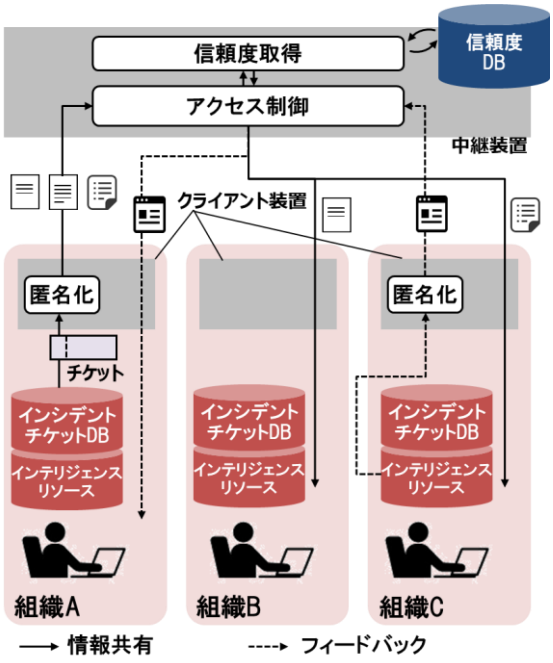

図1 提案手法の概要図

次に，信頼度について述べる．信頼度は情報共有時に秘匿レベルを決定するために用いられる値である．信頼度 DB に記録されている信頼度は，組織間の信頼関係や取引実績によって定まるシステム加入時の信頼度の初期値に，情報共有時の実績を反映した値である．例えば，フィードバックされたインテリジェンスがインシデント対処の役に立った場合，その評価を中継装置に送信し，中継装置は信頼度に一定値を加算する．

本システムは信頼度が低かった場合，情報共有における情報提供者の恩恵を評価し，これを参照して秘匿レベルを定める．例えば，この値が十分に高ければ，信頼度が低かったとしても秘匿レベルが低く、匿名化されていない情報を送信する．この値は，共有するチケット情報と，情報共有先組織が保持する情報の類似度から求められる．類似度が高ければ，チケット情報を共有した後フィードバックされる情報が，情報共有する組織に対して恩恵のある情報である可能性が高くなる．したがって，共有する情報と共有先の組織が持つ情報の類似度を用いることで，情報共有における恩恵を推定することができる．

本稿で述べるシステムでは，秘匿情報検索技術を用いて類似度を算出する．これは，情報を公開せずに類似度を評価する必要があるためである．チケット情報から検索クエリを作成し，これをクライアント装置に送信する．クライアント装置は，これを受信すると秘匿情報検索を実行し，類似度だけを返す．

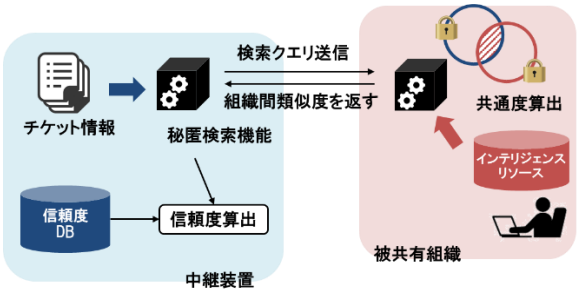

図2 情報共有時の信頼度算出処理

4. 今後の課題

本方式で実装したインシデントチケット共有システムを用いて，慶應大学の SOC が持つインシデントチケットを日立製作所へ共有した．今後は，チケット情報の共有にかかる時間を測定し，一般的な SOC が外部組織への定期連絡にかける時間の 10%である 180 秒と比較して，充分短いかどうか評価する．また，共有されたチケット情報をもとに対処の自動化を目指す．

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," 2011. [Online]. Available: http://www.ipa.go.jp/files/000024542.pdf

[2] 近藤 賢郎, 他, "分散 SOC 型 SOC アーキテクチャに基づいた複数組織間におけるセキュリティオペレーションの連携", マルチメディア, 分散協調とモバイルシンポジウム 2018 論文集, 2018,872-878, 2018

[3] S. N. Khajeddin, A. Madani, H. Gharaee and F. Abazari, "Towards a Functional and Trustful Web-based Information Sharing Center," 2019 5th International Conference on Web Research (ICWR), 2019, pp. 252-257, doi: 10.1109/ICWR.2019.8765297.

[4] 一般財団法人 運輸総合研究所, "サイバー攻撃に対するセキュリティ情報共有組織（ISAC）の構築に関する調査研究", 2018. [Online]. Available: https://www.jttri.or.jp/pdf/H29cyber_ISAC-houkoku.pdf