L-003

リジリエントセキュリティエンジンによるセキュリティオペレーションの改善

A improvement of security operation by Resillient Security Engine

野村公輝 † Kouki Nomura
永渕幸雄 † Yukio Nagafuchi
村田哲彦 † Tetsuhiko Murata
太田賢治 † Kenji Ota
向山明夫 † Akio Mukaiyama
張一凡 † Iifan Tyou
長山弘樹 † Hiroki Nagayama
小山高明 † Takaaki Koyama
谷川真樹 † Masaki Tanikawa

1 はじめに

近年，様々なクラウドサービスが存在しており，クラウドセキュリティサービスは，セキュリティの重要性が高まる中で，ユーザが簡単にセキュリティを導入できることで重要な位置を占めてきている．クラウドセキュリティサービスは，ユーザが簡単に利用できる反面，オペレータは，各テナントごとにセキュリティポリシーやセキュリティ機器が異なるためセキュリティインシデント発生時の対応が複雑であり，対処に時間がかかる等の課題がある．

これらの課題の解決に向け，我々は，セキュリティオペレーションの自動化を行う，リジリエントセキュリティエンジン（以降，“RSE”：Resillient Security Engine）[1][2] を開発した．本稿では，クラウドセキュリティにおけるセキュリティインシデント発生時のオペレーションの自動化，様々なセキュリティ機器の制御による RSE の利用例を提示する．

2 セキュリティオペレーションの課題

2.1 インシデント通知の課題

クラウドセキュリティでインシデントを検知した際のオペレータへの通知に関する課題を下記に提示する．

- 検知が不要あるいは誤検知のインシデント確認に稼動が必要
- 検知が不要あるいは誤検知であるインシデントが大量に通知されると，確認が必要なインシデントを見落とす可能性が存在

2.2 インシデントへの対処の課題

インシデント通知を受領したオペレータが実施するオペレーションを下記に提示する．

- セキュリティ機器から攻撃・脅威の検知ログを収集
- 攻撃・脅威の種別および最適な対処方法を判断
- ネットワークの構成情報に基づき FW 等の最適な対処機器を確認し，該当機器に制御命令を指示することでインシデントに対処

上記のオペレーションにおける課題を下記に提示する．

- テナント数の増加に従い，インシデント発生元の特定，遮断が煩雑
- テナントごとにセキュリティ機器のメーカ（管理ツール）が異なると，複数の管理ツールを操作するスキルが必要
- インシデント発生元の特定・遮断を手動で実施する場合，時間がかかる上に操作ミスの可能性が存在

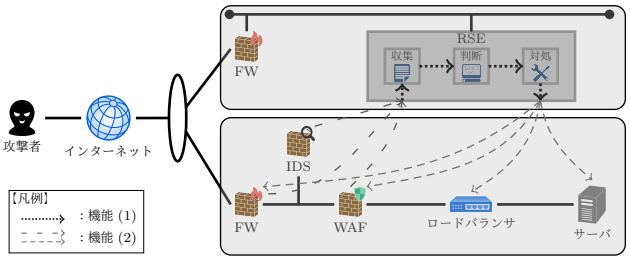

図 1 RSE

3 RSE

RSE は，多種多様なセキュリティ機器が出力するログを収集し，ログを事前に設定しておいたシナリオに従い処理することで，対処方法を判断し，オペレータへ対応策を提案したり，自動的にセキュリティ機器やネットワーク機器を制御するシステムである．処理の自動化によりオペレータの負荷を軽減することができる．

2 章で提示した課題に対して利用する RSE の機能について図 1 を使用して下記に提示する．

機能 (1) 自動化

RSE による自動化により，インシデント発生時における収集，判断，対処のオペレーションを迅速かつ正確に実行することができる．

機能 (2) 複数機器の制御

RSE による複数機器の制御は，多種多様なセキュリティ機器から攻撃・脅威の検知ログを収集し，攻撃・脅威の種別および最適な対処方法を判断した上で，複数の最適な機器で対処することで攻撃に対応する．

† 日本電信電話株式会社 NTT セキュアプラットフォーム研究所

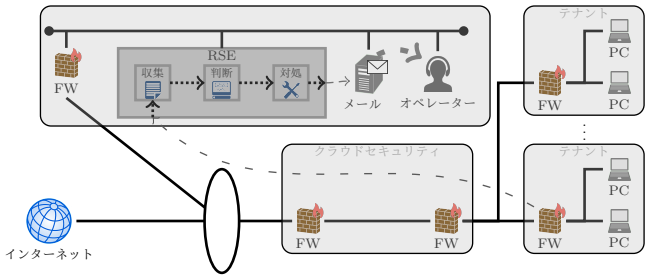

図 2 通知が不要なインシデントの通知防止

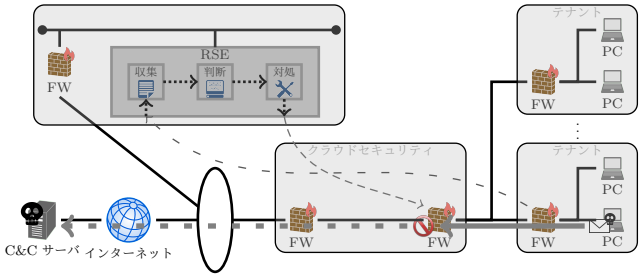

図 3 テナントからの不正通信の遮断

4 RSE の利用例

4 章では，3 章で提示した RSE の機能によりクラウドセキュリティにおける課題を解決する利用例を提示する．

4.1 通知不要なインシデントの通知防止

検知が不要，あるいは誤検知であるインシデントの通知が大量にある場合の利用例を提示する．

セキュリティ機器がインシデントを検知し，メール等からインシデントをオペレータに通知する．このとき，検知が不要，あるいは誤検知であると分かっているインシデントは，オペレータに通知されないことが望ましい．（検知したインシデントを条件に応じて通知しないといった対処ができるかどうかはセキュリティ機器により異なるため，セキュリティ機器によっては RSE を利用せずに対処可能である．）

RSE により通知が必要なインシデントのみをオペレータに通知する流れを図 2 を使用して下記に提示する．

1. セキュリティ機器により，インシデントを検知
2. RSE により，セキュリティ機器が検知したインシデントのログを収集
3. RSE により，検知したインシデントについてオペレータへの対処内容（通知要否）を判断し，対処を実行
4. RSE により，メール等からオペレータに通知が必要なインシデントのみを通知

上記では，3 章の機能 (1) を利用しており，インシデント確認に稼動が必要，確認が必要なインシデントを見落とす可能性が存在，といった 2.1 章の課題を解決できる．

4.2 テナントからの不正通信の遮断

テナント内の端末が標的型メール等によりマルウェアに感染した場合の利用例を提示する．

マルウェアに感染した端末は，インターネット上の C&C サーバへコネクトバック通信を試行し，コネクションの確立後に C&C サーバから遠隔操作されるため，コネクトバック通信を遮断することがサイバー攻撃からの防衛に有効である．

RSE によりコネクトバック通信を遮断する流れを図 3 を使用して下記に提示する．

1. テナント内の FW の Web フィルタ機能により，感染端末から C&C サーバへの通信を検知
2. RSE により，FW が検知した通信のログを収集
3. RSE により，検知した通信への対処内容を判断し，対処を実行
4. RSE により，テナントの上位階層にあるクラウドセキュリティの FW に通信遮断（HTTP ポート遮断）を指示

上記では，3 章の機能 (1)，(2) を利用しており，インシデント発生元の特定，遮断が煩雑，複数の管理ツールを操作するスキルが必要，時間がかかる上に操作ミスの可能性が存在，といった 2.2 章の課題を解決できる．

5 おわりに

本稿では，クラウドセキュリティにおけるセキュリティオペレーションの課題の解決のため，RSE の利用法を提案した．

今後，クラウドセキュリティに限らず様々なセキュリティオペレーションにおける課題の解決を目指した研究開発を実施する．

参考文献

[1] 小山 高明・波戸 邦夫・北爪 秀雄・永渕 光弘：サイバー攻撃から早期回復を図るリジリエント・セキュリティ技術，NTT 技術ジャーナル，Vol.26，No.3，pp.63-66，2014.

[2] 小山 高明・胡 博・永渕 幸雄・塩治 榮太朗・高橋 健司：グローバルな脅威情報基盤を用いたセキュリティオーケストレーションの実現，NTT 技術ジャーナル，Vol.27，No.10，pp.23-26，2015.