デジタルプラクティス　Vol.9 No.3 (July 2018)

特集招待論文

Security Operation Center構築とセキュリティ監視運用の取り組み

福本 佳成[1]　鈴木 武[1]　田代 正明[1]

[1]楽天（株）

楽天は1997年の創業以来，会員数・流通額・提供サービス数を急速に拡大させており，さらには楽天市場を中心とする楽天グループのサービスはGlobal化も加速し，現在ではさまざまな国でRakutenブランドを活用したインターネットサービスを展開している．楽天のサービスが急成長し，そのブランド認知度も上がる一方，攻撃者視点では楽天は格好の標的でもあり，インターネットサービスのセキュリティ対策は重要課題である．本稿では楽天のインターネットサービスでのセキュリティ対策全体から見るSOCの役割について言及するとともに，15年に渡るSOC運用経験からの監視システム技術の変遷とセキュリティ監視運用での留意事項について紹介を行う．

1. はじめに

インターネットが広く普及し，日常生活でのインターネットサービスの活用はもはや必要不可欠なものである．インターネット経由でオンラインショッピングなどさまざまなサービスが提供される中，犯罪標的も物理的制約のないインターネット環境へとシフトしている．そのサイバー攻撃は国境に関係なく日常的に行われており，その被害も後を絶たない．

インターネットサービス事業者にとっては自社サービスをサイバー攻撃から自衛することは事業継続において重要課題である．楽天においてもインターネットサービスのセキュリティ対策は創業間もない頃から継続して重要課題として取り組んできた．

この課題解決のための1つの取り組みとして，2003年に楽天グループ内のサービスを対象としセキュリティ監視を担うSOC（=Security Operation Center）を発足した．

本稿では，楽天におけるインターネットサービスのセキュリティ対策，特にSOCに焦点を当て事例とともに紹介する．第2章では楽天のセキュリティ対策の全体像を述べ，第3章では楽天におけるSOCの位置づけと目的を解説する．第4章では楽天の監視システム構成とその変遷を紹介する．第5章ではセキュリティ監視にかかわる外部環境の変化，第6章では社内の組織環境の変化について述べる．第7章ではセキュリティ監視運用業務における重要課題について言及する．

2. 楽天におけるセキュリティ対策の全体像

2.1　楽天のインターネットサービス

楽天はインターネットサービス企業であり，そのサービスのほとんどはインターネットを通じてユーザに提供されている．1997年にオンラインショッピングモールの楽天市場のサービス提供を開始して以来，その会員数・流通額を急速に伸ばしており，2012年には楽天市場での年間流通総額は1兆円を突破した[1]．また，楽天のサービスはオンラインショッピングモールにとどまらず，インターネットポータルサイトやオンライン旅行サービス，オンライン証券やクレジットカード，インターネットバンキングなどの金融系サービス，さらには電子書籍サービスやメッセンジャーアプリ，MVNOサービスなども含め，実に多種多様なインターネットサービスを展開しているコングロマリットな企業である．さらには楽天市場を中心とする楽天グループのサービスはGlobal化も加速し，現在ではさまざまな国でRakutenブランドを活用したインターネットサービスを展開している．

また，楽天のサービスが急成長し，そのブランド認知度も上がるに伴い，攻撃者視点では楽天は格好の標的となっている．実際，楽天のSOCでは2017年10月から12月の3カ月間で約3,000万件のサイバー攻撃を観測した．攻撃者は常に楽天のサービスの脆弱性を探している．

このように，楽天においてインターネットは事業の根幹であり，インターネットサービスを守るためのセキュリティ施策は重要性を増している．以下，楽天におけるセキュリティ対策の全体像とそれを支えるセキュリティ組織体制について述べる．

2.2　セキュリティ対策とSOCの位置づけ

筆者らは，2003年に楽天のセキュリティ対策を行った．楽天はサービス開発・運用をほぼ自社で行うことから，**図1**に示す通り，開発のセキュリティプロセスと運用のセキュリティ対策，大きく2つのセキュリティ対策のアプローチをとる．

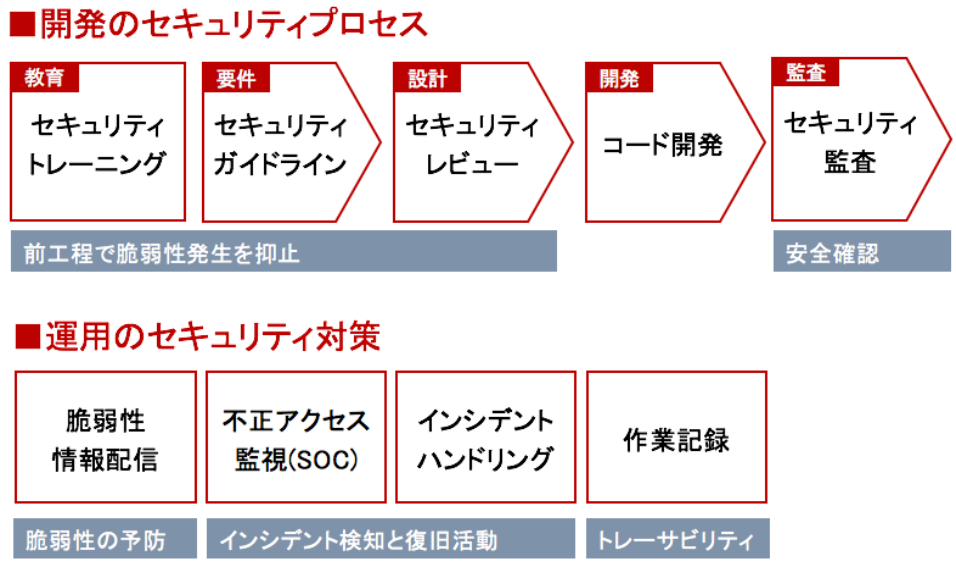

図1　2003年に考案したセキュリティ対策

開発のセキュリティプロセスでは，ソフトウェアセキュリティのリリース前にシステムから脆弱性を排除することを目指す．特に重点を置いているのが，開発プロセスでの開発者が脆弱性を作り込まないためのセキュアコーディング，監査プロセスでの，システムの脆弱性を徹底的に検証，および修正である．

運用のセキュリティ対策は，脆弱性の予防，インシデントの検知と復旧活動，トレーサビリティからなる．まず脆弱性の予防として，サーバソフトウェアのセキュリティレベルを維持するパッチマネジメントのための脆弱性情報の収集および分析業務を行う脆弱性情報配信がある．次に，インシデントの検知と復旧活動として，システムへのアクセス状況や機器の状態を監視する不正アクセスの監視と，不正アクセスや機器異常が発見された場合のインシデントハンドリングを行っている．

特に，前者の開発のセキュリティプロセスに重きを置き，開発者が最初から脆弱性のないシステムをつくることがセキュリティ対策の基礎と考えている．

2.3　セキュリティ組織体制

楽天では，セキュリティ対策を強力に推進するために，セキュリティ体制の強化にも努めてきた．楽天には，多数のセキュリティ専任のエンジニアが在籍している．また， Globalの主要拠点にもセキュリティエンジニアが配置されており，常に楽天グループのインターネットセキュリティ問題を収集し，問題発生時にはその原因調査，解析等を行っている．

楽天ではセキュリティ体制の1つとして早い段階でCSIRT（=Computer Security Incident Response Team）の構築を行った． CSIRTとは，コンピュータやネットワーク上でセキュリティ問題が起きていないかを監視し，万が一問題が発生した場合にその原因調査，解析を行ったりする組織の総称である．前節の楽天の運用セキュリティ対策においては主にインシデントハンドリングを担う．

外部セキュリティ組織と連携したインシデント対応を可能とするため，既存のセキュリティチームを正式にRakuten-CERT[2]と定義し，2007年12月に日本シーサート協議会[3]に加盟，翌年にはFIRST（=Forum of Incident Response and Security Teams）[4]にも加盟した．

セキュリティチーム発足当初は規模が小さく，セキュリティ会社へのアウトソース依存度が高かった．組織規模が大きくなるに伴いアウトソース比率は下げ，現在では，ほぼすべてのセキュリティ業務を自社のセキュリティエンジニアによって遂行している．これは，ある程度の組織規模となると，アウトソースするよりも自社のセキュリティエンジニアでセキュリティ対策をする方がメリットが大きいためである．たとえば，発注プロセスがないためフレキシブルかつ迅速なセキュリティ対応が可能であり，また全体的な対策コストについても改善される．

セキュリティ組織を発展させていくためには，優秀なセキュリティ人材の確保は大きな課題である．楽天は国内発のOWASP（=Open Web Application Security Project）のCorporate Supporter[5]になり，セキュリティコミュニティでの貢献により採用ブランドを向上させ，また，大学に楽天寄付講座を持ったりするなど，セキュリティ人材の採用強化のための活動も行っている．

以降の章では，運用のセキュリティ対策として不正アクセスの監視を行うSOCについて述べる．

3. 楽天におけるSOCの位置づけと目的

楽天においてのSOCへの期待は，第2章に挙げた複合的なセキュリティ対策の中でのセキュリティ監視機能であり，これまでの運用経験も含め期待される成果を出し続けている．

主な業務として，システムの不正アクセスを検知するためのIDS（=Intrusion Detection System）機器の運用，シグネチャの設定といった運用業務，アラート発生時の分析業務がある．分析の結果セキュリティインシデント調査が必要な際には前述のRakuten-CERT緊急連絡を行う． Rakuten-CERTによって対応が行われる．

楽天におけるSOCの主要な役割は，システムに脆弱性がなく，正しく守られているかを確認するベンチマークである．第2章で言及した通り，楽天では開発者が最初から脆弱性がないシステムを作ることがセキュリティ対策の基礎と考えており，システムの脆弱性はリリース前に徹底的に検証，および修正がなされている．SOCの検知がトリガーとなるセキュリティインシデント調査は，実際の結果は攻撃成功ではなく，ほとんどが誤検知である．

頻度はそれほど多くはないが，深刻な脆弱性が公表されてから間もない攻撃を検知することでシステムへの侵入を防いだ実績もあり，システムに潜在する脆弱性を悪用されてないか監視という意味においても，SOCは必要不可欠なセキュリティ対策であると位置づけている．

以下の章で，SOCを取り巻く環境の変化およびそれに伴うシステム構成，業務，人員の変遷について述べる．

4. 監視システム構成とその変遷

楽天ではSOCの監視デバイスはIDSとして利用しており，IPS（=Intrusion Prevention System），またはWAF（=Web Application Firewall）による防御機構を基本採用していない．これは，防御についてはアタックベクターとなる脆弱性そのもの，つまり問題の根本を排除するソフトウェアセキュリティでの対策こそが最も安全かつ確実なアプローチであり費用対効果も高いと考えるからである．脆弱性のない状態のソフトウェアであれば，IPSやWAFで防御する必要もなく，限りある予算とリソースは効果の高いセキュリティ対策に極力集約すべきである．

4.1 試験導入（2002）

楽天のインターネットサービスのセキュリティ監視は，2002年にオープンソースのIDSを試験的に導入したことに始まる．当時はApacheやOpenSSLなどにリモートから直接システムに侵入されるような深刻な脆弱性も多々あり，また，当時の楽天はセキュリティ対策全般がまだ成熟していなかったため，この試験的なIDS導入は楽天のサービスへのサイバー攻撃の状況を可視化しシステムを守るための成果を上げた．

4.2 導入初期（2003〜）

SOCへの本格的な投資が意思決定され，セキュリティベンダのSOC，商用IDSを活用した24/7（24時間365日対応）のセキュリティ監視業務がスタートした．**図2**に当時のシステム構成の概要を示す．IDSは一番容易にトラフィックをキャプチャできるポイントに設置し，トップルータとISP間のトラフィックの複製を監視した．当時はSSLアクセラレータがまだ主流ではなくすべてのトラフィックを平文でキャプチャすることが困難であったこともあり，網羅性に課題があると認識をしつつ，このような構成で監視をスタートさせた．

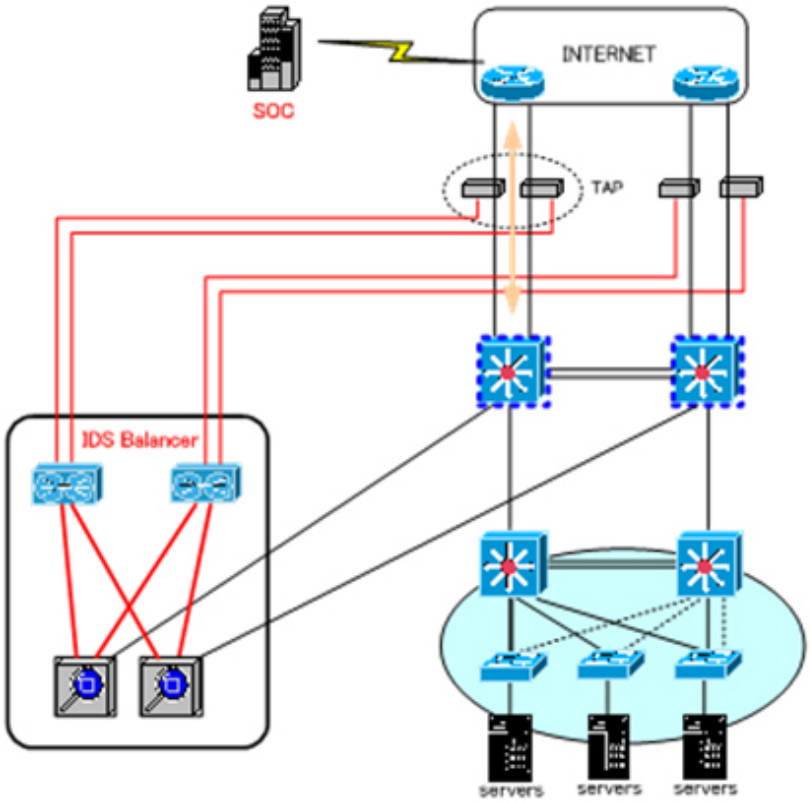

図2　2003年のシステム構成図（一部抜粋）

また，当時のIDSでは大量のトラフィックを解析できる処理能力はなく，過負荷時のイベント検知に関するシステム障害も多かったため，本構成を実現するためにIDSロードバランサによって負荷分散を行っていた．

4.3　最新世代（2013〜）

導入から数年が経ち，SSLアクセラレータの利用が標準となり，監視するトラフィックのキャプチャポイントは徐々にロードバランサの下になり，最終的にはすべて平文のトラフィックを監視できるようになった．**図3**に最新世代の監視構成を示す．

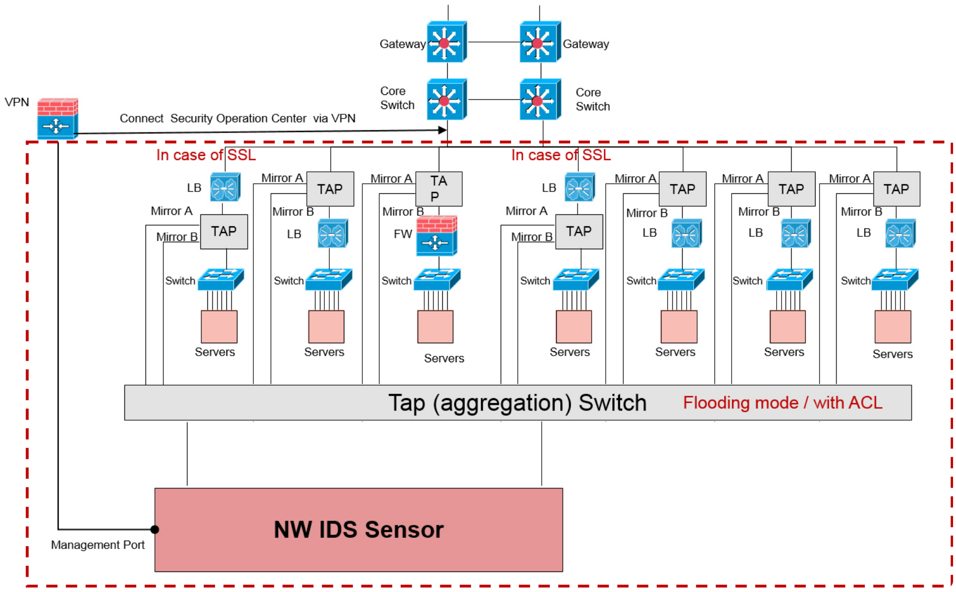

図3　2013年のシステム構成図（一部抜粋）

トラフィックのキャプチャポイント以外でも大幅なシステム構成の変更があった．IDSの大幅なパフォーマンスの向上により当初導入していたIDSロードバランサによる負荷分散が不要となった．逆にポート数の多いスイッチに複製したトラフィックを集約してミラーポートでまとめてハイパフォーマンスのIDSに流す構成となった．

このように，楽天では機器の進化に合わせ，SOCのシステム構成を変化させている．SSLアクセラレータの標準化，そしてIDSのパフォーマンスの大幅な向上は，SOC監視構成にとって大きな影響を与えた．一方で，IDSはIPSとしての機能を十分持ち合わせるようになったが，楽天ではその防御の機能は活用していない．楽天の防御の方針は，今でも本質的な問題解決として脆弱性そのものをなくすこととしているからである．

5. 外部サービスの利用によるセキュリティ監視運用業務の複雑化

楽天のシステム構成は自社構築のみのシステム構成だったが，近年では外部サービスも活用が増えている．これに伴い，セキュリティ監視運用業務が複雑化している．外部サービスの活用によるSOCでのセキュリティ監視運用業務の複雑化についてCDN（=Content Delivery Network）およびパブリッククラウドの利用から述べる．

CDN利用時の，セキュリティ監視運用上のケースは大きく2つある．

1つ目は，CDN側で受けている攻撃の通信は，設定上正しい通信ではない場合に，オリジンサーバにリクエストが届かないため，SOC側としてはサービス全体を俯瞰したサイバー攻撃の分析がより難しくなることである．

2つ目は，攻撃の通信がCDN側の設定上問題なく，オリジンサーバにコンテンツを取りに行く場合において，CDNとの契約内容やSOCベンダの仕様によっては**図4**に示すように攻撃者の送信元IPアドレスをSOC側で直接確認できないことである．その際，攻撃元の調査を行う場合においては，SOCから連絡を受けて，それを元に楽天側からCDN側に問合せを行う必要があり調査に時間がかかる．

これら，攻撃の全体像が把握しにくくなること，セキュリティベンダのSOCの仕様によって送信元IPアドレスの調査に時間がかかってしまうこと，これらの2点のデメリットは運用上許容できるかどうか留意が必要である．

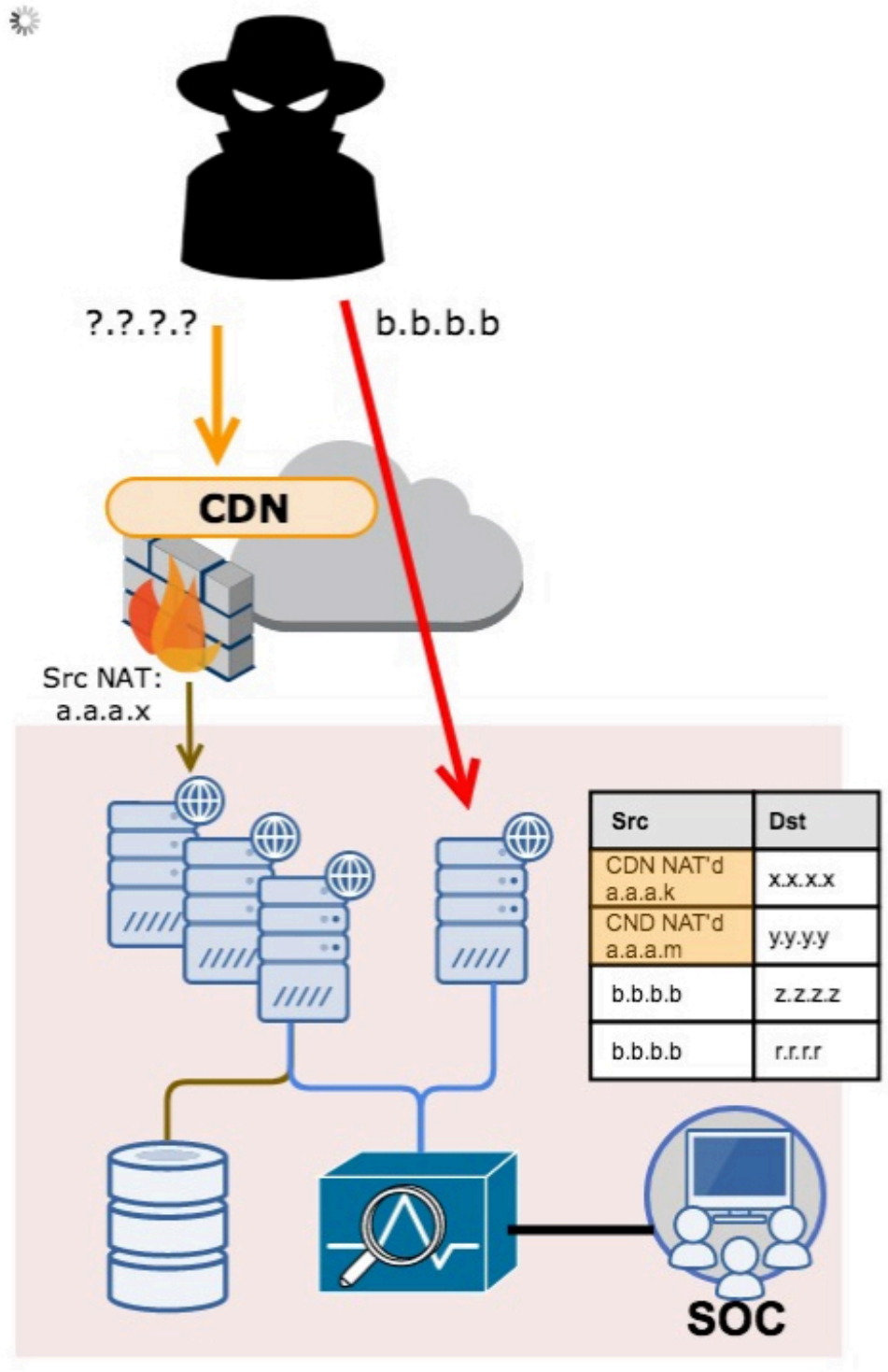

図4　SOC側では攻撃者のIPアドレスが不明

また，CDN側のセキュリティ機能を使って自社で直接送信元IPアドレス，攻撃の調査ができた場合においても，調査のためのセキュリティ管理ツールが増えることとなり，セキュリティインシデント調査対応フローの複雑化をもたらしている．

また，パブリッククラウドの活用でも同様の課題がある．楽天は自社のデータセンターに加え，一部はパブリッククラウドも活用してインターネットサービスを運営している．そのパブリッククラウド側でのセキュリティ監視システムのテクノロジーについては，これまで利用していたオンプレミスのセキュリティアプライアンスは使えないため，パブリッククラウド環境専用のセキュリティ監視サービスを別途追加で選定する必要があった．

外部サービスを利用する場合のセキュリティ監視運用では，上記で述べた運用上の複雑性の課題があり，また，セキュリティ監視情報を一元管理することも難しくなっている．常に進化していくテクノロジーによって状況は変化しており，柔軟に業務を変化させていく必要がある．

6. 人員の変遷 アウトソースからインハウスへ

楽天では，前章で述べたセキュリティ監視対象，運用の複雑化，社内組織環境の変化に対応するため，SOCのアウトソースからインハウスへの切り替えを行った．

社内組織環境の変化としては，2010年に発表した楽天の社内公用語の英語化，そしてエンジニアの多国籍化がある．また，2014年にはインドにも新たな開発，運用拠点を設置し，楽天グループのシステム開発から運用業務を一貫して実行できる体制整備が進められていた．拡大する世界各国の楽天グループのサービスに対するサイバー攻撃の可視化，攻撃検知から影響分析，対応までの時間短縮も課題となっていた．

インハウスへの移行判断を行った大きなポイントは，監視チームが社内の構成情報，システムログ等へアクセスすることによって，誤検知切り分けをこれまで以上に踏み込んで行えることである．アウトソースでは，IDSのログだけでは誤検知切り分けのエビデンスとして十分ではなく，切り分けのための調査の多くを楽天側で実施せざるを得ない状況にあった．

上記のようなセキュリティ監視対象，運用の複雑化，グローバル化などの変化に柔軟に対応していくために，インハウスでカスタマイズできることが必要と判断しインハウスへの移行が実施された．

2017年，楽天はインドの運用拠点をセキュリティ監視の中心として自社でSOCを構築し，柔軟な監視体制を実現した．アウトソースベンダからインハウスの基盤への切り替えは事前の計画に従い，段階的に実施され大きな問題もなく完了した．

アウトソースからインハウスに移行する際，大量のセキュリティイベントの効率的な収集・解析，セキュリティツールも活用した調査・検証，チケット管理，そのためのさまざまなツールが必要となるが，楽天ではオープンソースの活用によって自社のSOC運用環境を実現した．Graylog[6]のようなログ管理ツールを中心とするオープンソースツールの発展，およびそれらの社内での浸透が，柔軟性の高いセキュリティ監視システム基盤の構築につながった．

まったく問題がなかったわけではなく，監視運用業務当初は事前の想定を上回る大量のセキュリティイベントの処理の問題，セキュリティイベント解析担当者のリソース配置等の問題に直面した．こうした問題には，システムのチューニング，イベント処理の優先度，リソース配置計画の変更等の対応を行うことで対処した．

また，セキュリティ監視運用の品質を保つためには，これまで以上に継続的な採用活動や人材育成にも注力しなければならない．自社SOCを維持するための投資を移行後も継続的に行っている．

7. セキュリティ監視運用業務における重要課題

セキュリティ監視運用業務において特に重要なことは，24/7体制で開発・運用部隊と連携したセキュリティインシデント対応運用業務である．このインシデント対応業務を実現・維持するためには，インシデント対応体制・フロー整備，インシデント調査対応力を向上させるトレーニング，イベント時期によるインシデントの発生頻度の上昇に対する備えが求められる．楽天では以下のように対処している．

インシデント対応体制・フローとして脆弱性を悪用した攻撃が成功した可能性のある緊急連絡に対して，24/7体制で調査対応が行われるフローを整備している．これが実施できなければSOCによるセキュリティ監視機能を十分に活用できているとはいえない．特に脆弱性が公表されてから間もない攻撃のケースにおいては即時対応ができなければ監視対象のシステムをサイバー攻撃から防ぐことは困難である．実際，今年（2018年）3月に発生したApache Struts 2[7]を悪用した攻撃（CVE-2017-5638[8]）では，脆弱性公表とほぼ同時に攻撃コードが公開され，ワークアラウンドやバージョンアップ対応前の攻撃が危惧されたが，SOCによる監視によって実際に攻撃を受けたサーバを即刻サービスアウトして脆弱性対応した．深夜の時間帯の対応であったが，24/7の対応フローのおかげで被害を未然に防ぐことができた．

インシデント調査対応能力を向上させるためには，開発・運用を担当しているエンジニアにセキュリティトレーニングを実施することは重要な要素である．セキュリティ知識が十分でなければ，速やかな調査や正確な脆弱性対応は行えない．そのため，楽天では自社のCSIRTであるRakuten-CERTのみならず，すべてのエンジニアに職種に合ったセキュリティトレーニングを受講することを義務付けている．セキュリティ業務はセキュリティエンジニアだけではできない．関連するエンジニアすべてが一定のセキュリティ知識を持つことが大事である．

イベントの時期によるインシデント発生頻度の上昇への対応も求められる．経験上ではあるが，夏季休暇などの長期休暇中のセキュリティインシデントの発生頻度は平日に比べると非常に高く，注意が必要である．推測ではあるが，攻撃者も休暇中は攻撃するための十分な時間がある，もしくは担当者不在を意図的に狙っている可能性があると考えられ，攻撃者側での攻撃頻度が高まるタイミング，もしくは守り側の休暇中の隙を狙う攻撃者の行動には十分に警戒をしなくてはならない．常に攻撃が来るという意識を持つことと，そしていつでも必ず連絡が取れる運用設計が必要である．

8. おわりに

本稿では，楽天におけるSOC構築，運用の経験から，実際のSOCの活用事例，セキュリティ監視システムの技術的な動向やセキュリティ監視運用業務での注意点を述べた．テクノロジーの変化に伴い，セキュリティ監視システムも変化に対応していかなければならない．楽天の場合はサービスが急成長しているステージであり，新しいテクノロジーも積極的に取り入れているため，特にその点は重要である．

また，サイバー攻撃の件数は劇的に増加しており，実際，楽天市場のトップページの約30%のトラフィックは不正目的のボットによるアクセスである．攻撃者は常に我々のインターネットサービスのセキュリティの隙を狙っており，いかに不正アクセス監視業務をAIなどで自動化していくかが次の重要な改善のテーマである．

そして，最後はやはりセキュリティエンジニアと開発・運用者との連携したセキュリティインシデント対応であり，そこは対応スキルも含めた十分な体制を整備し，引き続き有事に備えたい所存である．

謝辞 本稿を執筆するにあたり，楽天（株）テクノロジープラットフォーム統括部の吉岡弘隆氏，楽天（株）楽天技術研究所の平手勇宇氏に，多大な助言とサポートをいただきました．ここに感謝の意を表します．

参考文献

1）楽天市場の年間流通総額が1兆円の大台を突破，
https://corp.rakuten.co.jp/news/press/2012/1029_02.html
2）コンピュータ関連事故の対応組織「CSIRT」を新設，
https://corp.rakuten.co.jp/news/press/2007/1206_1.html
3) 日本シーサート協議会，http://www.nca.gr.jp/outline/index.html
4）FIRST，https://www.first.org/about/
5）OWASP Corporate Supporter Bios，
https://www.owasp.org/index.php/Corporate_Supporter_Bios
6）Graylog，https://www.graylog.org/
7）Apache Struts 2，https://struts.apache.org/
8）CVE-2017-5638 Detail，
https://nvd.nist.gov/vuln/detail/CVE-2017-5638

福本 佳成（非会員）yoshinari.fukumoto@rakuten.com
インターネットセキュリティ専門会社でセキュリティプロダクトの研究開発を経て，2002年に楽天（株）に入社．楽天グループのインターネットサービスのセキュリティを担当．主には安全なソフトウェア開発の推進とセキュリティ運用を担当している．2007年にRakuten-CERTを設立．Rakuten-CERT Representative．活動開始時よりOWASP Japan Advisory Boardを務める．東京工業大学サイバーセキュリティ特別専門学修プログラム特定教授．近年はサイバー犯罪対策にも注力している．

鈴木　武（非会員）takeshi.a.suzuki@rakuten.com
2010年に楽天（株）に入社．インターネットサービスのセキュリティ運用監視，脆弱性管理を担当．現在はRakuten Europe S.a.r.l. にてヨーロッパ楽天グループ会社のセキュリティ対策推進に従事．CISSP, CISA.

田代　正明（非会員）masaaki.tashiro@rakuten.com

2012年楽天（株）に入社．セキュリティオペレーション，社内ITセキュリティ，PCI DSS監査，およびCSIRT業務に従事し2017年の社内SOCへの監視運用業務切り替えを担当．

投稿受付：2018年1月25日
採録決定：2018年4月23日
編集担当：飯村結香子（NTT ソフトウェアイノベーションセンタ）