佐藤健一 | サイバーセキュリティエンジニア

日本、東京都、千代田区、東京都千代田区丸の内 1-2-3、100-0001
+81 90-1234-5678 • kenichi.sato@example.com • https://kenichi-sato.dev
@kenichi-sato • @kenichi-sato • @kenichi_sato

基本情報

セキュリティエンジニアとして 5 年以上の経験を持ち、ネットワークセキュリティ、脆弱性診断、インシデント対応に精通しています。特にペネトレーションテストとセキュリティアーキテクチャの設計に強みを持ち、金融機関や E コマース企業のセキュリティ強化に貢献してきました。チームをリードし、セキュリティ意識向上のためのトレーニングを実施した経験もあります。常に最新の脅威情報を追い、プロアクティブな防御策を提案することを心がけています。

学歴

東京大学 **https://www.u-tokyo.ac.jp**
修士、情報理工学系研究科コンピュータ科学専攻、成績：3.8/4.0 2013 年 4 月〜2015 年 3 月
情報セキュリティを専攻し、暗号プロトコルとネットワーク防御に関する研究に従事。修士論文では「機械学習を用いた異常検知による侵入検知システムの改善」をテーマに研究。**コース**：情報セキュリティ、暗号理論、ネットワーク工学、オペレーティングシステム、データベースシステム

職歴

株式会社サイバーディフェンス **https://www.cyberdefense.co.jp**
シニアセキュリティエンジニア 2019 年 4 月〜現在
- 金融機関向けのセキュリティアーキテクチャ設計と実装をリード
- 脆弱性診断およびペネトレーションテストを実施し、重大な脆弱性を複数発見□修正
- インシデント対応チームのリーダーとして、セキュリティインシデントの調査と復旧を指揮
- セキュリティポリシーの策定と従業員向けセキュリテイトレーニングを実施
- 最新の脅威情報を収集し、プロアクティブな防御策を提案

キーワード：ネットワークセキュリティ、ペネトレーションテスト、インシデント対応、セキュリティアーキテクチャ

株式会社セキュアテック **https://www.securetech.co.jp**
セキュリティエンジニア 2015 年 4 月〜2019 年 3 月
- Web アプリケーションの脆弱性診断を担当し、SQL インジェクションや XSS などの脆弱性を特定
- セキュリティ監視システムの運用と改善を実施
- セキュリティインシデントの一次対応と報告書作成
- 社内セキュリティガイドラインの整備に貢献

キーワード：脆弱性診断、Web セキュリティ、セキュリティ監視

言語

日本語：ネイティブ□母国語レベル **キーワード**：日本語ネイティブ
英語：完全な実務レベル **キーワード**：TOEIC 900 点、技術文書読解

スキル

ネットワークセキュリティ：エキスパート **キーワード**：ファイアウォール、IDS/IPS、VPN、パケット解析、ネットワーク設計
ペネトレーションテスト：上級 **キーワード**：Metasploit、Burp Suite、Nmap、Wireshark、Kali Linux
クラウドセキュリティ：中級 **キーワード**：AWS、Azure、GCP、IAM、セキュリティグループ

暗号技術: 上級　　**キーワード**: PKI、TLS/SSL、暗号化アルゴリズム、鍵管理

受賞□表彰

年間最優秀セキュリティエンジニア賞
株式会社サイバーディフェンス　　2022 年 12 月
金融機関向けのセキュリティプロジェクトにおける卓越したリーダーシップと技術的貢献に対して授与。

セキュリティ研究優秀賞
東京大学　　2015 年 3 月
修士論文「機械学習を用いた異常検知による侵入検知システムの改善」が高く評価され授与。

資格□免状

CISSP（情報システムセキュリティ専門家）　　**https://www.isc2.org/Certifications/CISSP**
(ISC)²　　2020 年 6 月

OSCP（Offensive Security Certified Professional）　　**https://www.offensive-security.com/pwk-oscp/**
Offensive Security　　2018 年 11 月

情報処理安全確保支援士　　**https://www.ipa.go.jp/shiken/kubun/sc.html**
情報処理推進機構　　2017 年 4 月

出版□著作

情報処理学会論文誌　　**https://www.ipsj.or.jp**
機械学習を用いた異常検知による侵入検知システムの改善　　2015 年 3 月
侵入検知システムの精度向上を目的として、機械学習アルゴリズムを適用した異常検知手法を提案。従来手法と比較して検知率が 15% 向上し、誤検知率が 20% 低減することを示した。

プロジェクト

セキュリティ監視ダッシュボード　　**https://github.com/kenichi-sato/security-dashboa**
複数のセキュリティログを統合し、リアルタイムで可視化するダッシュボード　　2021 年 1 月〜2021 年 6 月
- Elasticsearch、Logstash、Kibana (ELK スタック) を使用してセキュリティログを収集□分析
- 異常検知アラートを Slack に通知する機能を実装
- セキュリティ運用チームの効率を 30% 向上

キーワード: セキュリティ監視、ELK、ログ分析、可視化

興味□関心

CTF (Capture The Flag): Web、暗号、フォレンジック

読書: セキュリティ関連書籍、技術書

ボランティア活動

日本サイバーセキュリティコミュニティ　　**https://www.jcsc.org**
セキュリティトレーナー　　2018 年 4 月〜2023 年 3 月
- 初心者向けのセキュリティワークショップを定期的に開催
- CTF 大会の運営スタッフとして参加
- セキュリティ意識向上のための講演を実施