LS 研　2019 年度短期研究分科会　研究テーマ概要

No.	短期研究分科会テーマ
1	業務システムのデジタル化に向けたマイクロサービスアーキテクチャ適用検討
2	マルウェア対策に向けたエンドポイントとネットワークの適切な関係に関する研究
3	頻繁に変更が発生するセキュリティルールに関する効率的な管理手法の確立

No.1	**業務システムのデジタル化に向けたマイクロサービスアーキテクチャ適用検討**
研究内容・研究方針 （背景・現状の課題、研究目標・方向性）	デジタルビジネス時代において、小さなサービスを組み合わせてアプリケーションを開発することで変化対応力を高めるマイクロサービスアーキテクチャが注目されている。しかし、従来のモノリシック構造を前提としたウォーターフォール型開発とは異なる新しいアーキテクチャや開発スタイルであるため、適切な設計・開発手法、品質確保の考え方、運用上の留意点などのノウハウが整備されていないのが現状である。このため、不用意な適用はプロジェクトの失敗を招きかねないという課題がある。 本分科会では、マイクロサービスアーキテクチャの本質・特徴を理解した上で、近年急速な進歩を遂げている docker、kubernetes などのコンテナ技術や、品質確保のための自己回復性、サーキットブレーカー、カオスエンジニアリングなどの考え方、手法を調査し、マイクロサービスアーキテクチャ適用とシステム運用の考慮点について研究する。
目標とする研究成果	・マイクロサービスの特徴（長所と短所、投資効果、制約条件、課題など）を整理 ・企画／設計／品質確保における検討ポイント （適用可否指針、分割粒度、データ観点など） ・実装上必要となる基盤機能（CD/CI、クラウド環境など）の明確化
具体的な研究手順	(1) マイクロサービスに関する情報の収集、事例調査 (2) マイクロサービスの特徴の整理 (3) マイクロサービスを企画／設計／開発／運用するために考慮すべき検討ポイントのまとめ
参加条件 対象部門・クラス・前提スキルなど	・CD/CI やアジャイル開発またはリーンスタートアップの経験のある方 ・マイクロサービスの導入を検討している方

LS 研　2019 年度短期研究分科会　研究テーマ概要

No.2	マルウェア対策に向けたエンドポイントとネットワークの適切な関係に関する研究
研究内容・研究方針 （背景・現状の課題、研究目標・方向性）	従来の企業ネットワークでは、インターネットの入口・出口対策として、UTM などネットワークセキュリティ製品を適用し、トラフィックを検査することでマルウェアの侵入を防いできた。しかしながら、近年は常時 SSL（Always On SSL）、公衆無線 LAN の普及など、インターネットにおける SSL 暗号が増加傾向にあり、トラフィックが暗号化されていることでネットワーク上におけるトラフィックの検査は益々困難な状況になってきている。また、今後はインターネット・ブレイクアウトを指向する企業が増えると予想され、ネットワークによるマルウェア対策の考え方は変化することが予想される。 本分科会では、EDR※などエンドポイントソフトとネットワークによるそれぞれのマルウェア対策技術の価値と関係を整理し、マルウェア対策の考え方を研究する。 EDR: Endpoint Detection and Response（エンドポイントでの検出と対応）
目標とする研究成果	・エンドポイントソフトによるマルウェア対策と、ネットワークによるマルウェア対策の分類と価値の整理 ・企業ネットワークにおけるマルウェア対策の考え方
具体的な研究手順	(1) ネットワークによるマルウェア対策技術調査（分類、価値・効果と技術課題） (2) EDR といわれるエンドポイントソフト技術調査（分類、価値・効果と技術課題） (3) (1)(2)の比較検討 (4) 企業ネットワークにおけるマルウェア対策の考え方の提言
参加条件 対象部門・クラス・前提スキルなど	・ネットワーク構成設計に携わる方 ・マルウェア対策に取り組んでいる方、または検討されている方。

No.3	頻繁に変更が発生するセキュリティルールに関する効率的な管理手法の確立
研究内容・研究方針 （背景・現状の課題、研究目標・方向性）	現在、ISO27002・SP800-53・FISC 安全対策基準など、非常に多くのセキュリティ対策ガイドラインが存在し、日々その内容が更新されている。また、企業や組織において、セキュリティ事故が起こるたびに新しいセキュリティルールが追加されている。そうした中、レガシーセキュリティルール（古くなったセキュリティルール）の整理・統廃合が必要であるが、そのままの状態で放置されている現状が散見される。レガシーセキュリティルールを廃止することは、新規にルールを作るよりもはるかに多くのコストを必要とし、その成功例も少ない。 本分科会では、レガシーセキュリティルールの効率的な分析手法および成功事例のケーススタディなどを行い、効率的な管理手法を研究する。
目標とする研究成果	・レガシーセキュリティルールの評価手法（有効性、効率性など） ・レガシーセキュリティルールの廃止基準ガイドライン ・レガシーセキュリティルール管理手法
具体的な研究手順	(1)レガシーセキュリティルールを廃止した成功事例の収集 (2)事例の分析と KSF※の抽出 (3)レガシーセキュリティルールの廃止に必要な評価手法の確立 (4)上記を踏まえて、効率的な管理手法の検討 ※KSF=Key Success Factor の略称。事業の成功要因
参加条件 対象部門・クラス・前提スキルなど	・セキュリティ管理部門の方 ・業界団体から発行される基準・ガイドラインに詳しい方