2025年度
企業情報セキュリティ研究会
活動成果報告

部会長　本池　正人
（コープ情報システム株式会社）

要約　セキュリティ対策の高度化と実務課題

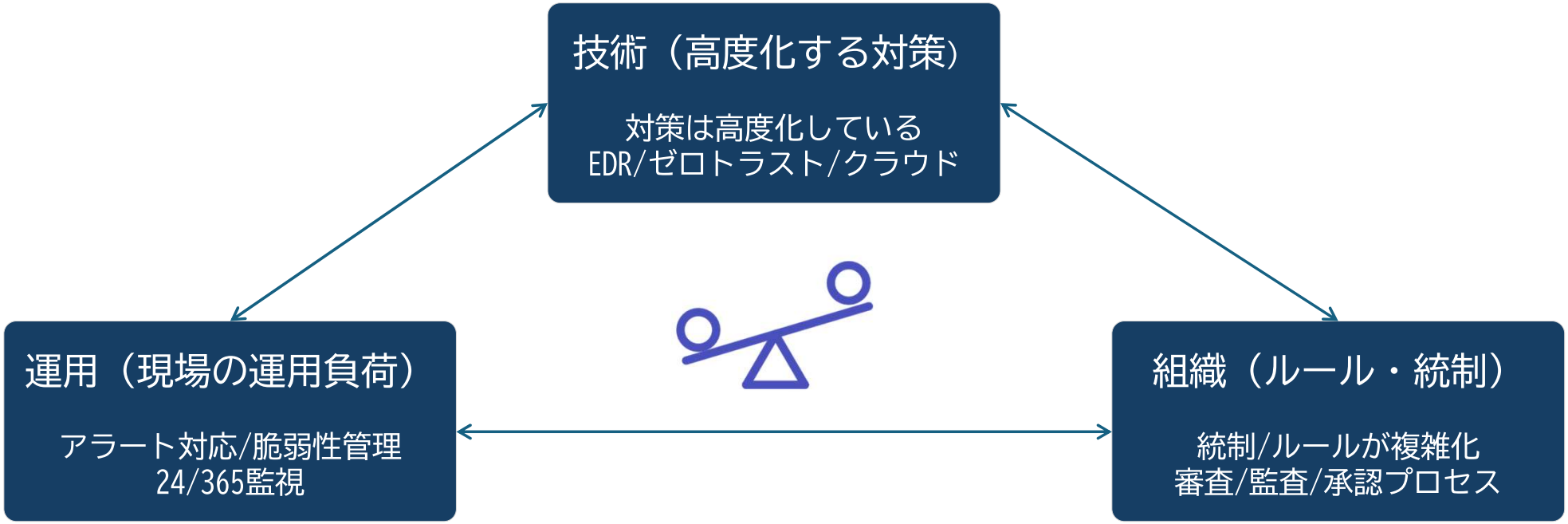
セキュリティ対策は高度化しているが、現場では運用の難しさが増している。

セキュリティ対策は急速に高度化	• EDR、ゼロトラスト、クラウドセキュリティなど • 新しいツール・仕組みが次々に登場
企業では導入が進んでいる	• 多くの企業で対策製品の導入は進展。 • 技術的な対策は着実に進化。
現場では新たな課題	• アラートの増加 • 運用の複雑化 • 人材不足／スキル不足

技術の高度化に対して、運用と組織のバランスが崩れている

要約　技術・運用・組織の構造課題

課題は、個別の製品や運用ではなく「技術・運用・組織」の構造的な歪みにある



問題は、「個別対策」ではなく、三者のバランス崩壊である。

本報告書の位置づけ

本報告書は、2025年度の企業情報セキュリティ研究会において行われた議論や情報共有の内容を整理したものである。

研究会では、参加企業の実務担当者が自社の取り組みや課題を持ち寄り、分科会および全体会において意見交換を行った。本報告書は、そこで共有された論点を整理し、企業の実務に資する形で広く共有することを目的として作成している。

本報告書で整理している課題は、特定の企業の成熟度や取り組みの水準を示すものではない。

セキュリティ対策の高度化やIT環境の変化に伴い、多くの企業に共通して生じている構造的な課題を整理したものである。
また、本報告書は特定の製品・サービス・対策手法の採用を推奨するものではなく、研究会での議論を整理したものである。研究会はチャタムハウスルールに基づき運営しており、個別企業の事例や発言内容が特定されない形で内容を整理している。

第1章
企業情報セキュリティ研究会の概要

本章では、本研究会の目的・特徴、構成および運営方法、参加企業の概要を示す

1.1 研究会の目的

- 背景

  セキュリティ対策の高度化やIT環境の複雑化により、企業におけるセキュリティ運用の負荷が増大している

- 企業情報セキュリティ研究会とは

  企業横断で情報セキュリティに関する実務課題を持ち寄り、議論する研究会

分科会	テーマごとに参加者が分かれ、実務事例や課題をもとに率直な意見交換を実施。参加者全員が発表に関わる形式とし、実務に基づく議論を重視
全体会	議論内容の共有・各分科会の代表者からの事例発表 外部講師によるゲスト講演

- 研究会の目的

  企業の実務課題を持ち寄り**「セキュリティ対策を企業の実務としてどう成立させるか」**という視点から議論を行い、実務的な示唆を整理する。

1.2 研究会の構成と運営体制

● 幹事団

部会長	本池 正人	コープ情報システム株式会社
副部会長	戸村 和宣	丸文株式会社
副部会長	荒尾 幸嗣	双日テックイノベーション株式会社
副部会長	西村 清翔	インフォテック株式会社

● 役割

幹事団	研究会全体の企画・推進
分科会長/副分科会長	分科会の運営・議論整理
参加者	議論のテーマ提示/議論への参加

● 運営方針

- チャタムハウスルールのもとで実施
- 率直な意見交換と実務知の共有を重視

1.3 分科会の活動テーマ

本研究会では、企業のセキュリティ課題を多面的に検討するため、三つのテーマの分科会を設けて議論を行った。

	研究テーマ	人数	分科会長	副分科会長
A	技術対策・最新トレンドの研究 最新の攻撃手法と対策、クラウド・AIの利用などに伴うリスクについて、企業における技術的対策のあり方について議論	16	東日本旅客鉄道（株） 鈴木	双日テックイノベーション（株） 荒尾
B	セキュリティ運用・インシデント対応 組織におけるセキュリティ管理・運用の実務やインシデント発生時の対応体制および対応プロセスの高度化について議論	16	（株）富士薬品 髙橋	NOK（株） 河本
C	セキュリティ戦略・組織強化 組織のセキュリティ体制の整備、運用の最適化、人材育成など、セキュリティマネジメントの強化について議論	18	（株）エイジス 川又	新電元工業（株） 松本

1.4 研究会の開催実績

本研究会は、2025年6月から2026年3月までの期間に、分科会・全体会で構成される研究会および分科会活動を含め計10回開催した。

2025/6/3　第1回研究会
・オリエンテーション
　（方針説明、分科会の開催日程調整）
・名刺交換会

2025/7/23　第2回研究会
・分科会討議
・分科会活動内容の報告
・ゲスト講演

2025/8　　分科会
・分科会ごとに開催
・分科会の討議

2025/9/26～9/27　第3回研究会
沼津合宿
・分科会討議
・分科会活動内容の報告
・IPAインシデントゲーム

2025/10,12,2026/2　　分科会
・分科会ごとに開催
・分科会の討議

2025/11/14,2026/1/23
2026/3/6　第4,5,6回研究会
・分科会討議
・分科会活動内容の報告
・ゲスト講演（11月のみ）

1.5 参加企業の構成、セキュリティ業務経験年数

本研究会には、**49社・50名が参加**した。製造、エネルギー、金融、食品、交通など**多様な業種の企業が参加した。**参加企業の多くは上場企業またはそのグループ企業であり、基幹産業を担う企業の情報システム部門および情報システム子会社を中心とした構成となっていた。情報セキュリティ業務の経験年数を見ると、**4年以上の実務経験者が過半数を占めており**、企業の現場でセキュリティ業務を担う担当者を中心とした構成となっていた。

業種	人数	※	備考
製造	14	3	
金融	6	3	
エネルギー	5	2	
交通	3	1	
食品	4		
総合エンジニアリング	2	1	
ITサービス	11		
その他	5	1	商社,小売・流通,人材サービス,棚卸,生協

セキュリティ業務経験年数	人数
4年以上	27
2～3年	12
1年	6
経験なし	5

（※）情報システム子会社

第2章
研究会で扱った課題

本章では、企業の情報セキュリティを取り巻く環境の変化と、実務の現場で共通して発生している課題を整理する。これらを踏まえ、本研究会が向き合った問いを明確にする。

2.1 セキュリティ対策・運用体制を取り巻く環境

近年、企業のIT環境は大きく変化し、セキュリティ対策の対象領域は急速に拡大している。

環境の変化

SaaS/IaaSなどクラウド利用の拡大	管理対象の増加・可視化の困難化
生成AIの業務利用	利用範囲の拡大と統制の難しさ
ゼロトラストネットの導入	認証・アクセス管理の複雑化
サプライチェーンリスクの増大	自社外を含めたリスク管理の必要性

現場の課題

セキュリティ専門人材の不足	対応が属人化し、継続的な運用が困難
監視・分析業務の増大	アラート対応に追われ、本来対応すべき事象を見落とすリスク
グループ会社・取引先への統制	統制のばらつきにより、全体としてのセキュリティ水準が不均一

継続可能なセキュリティ運用体制の確立が企業共通の課題となっている。

2.2 本研究会が向き合った問い

本研究会ではこうした構造的課題を踏まえて、次の問いを中心に議論を行った。

技術的な対策の導入自体は進んでいる
しかし、
運用・組織・業務との不整合により、
導入した対策が十分に機能していない

⬇

高度なセキュリティ対策を、
企業の実務の中でどのように機能させるか？

2.3 分科会Aで扱ったテーマ

テーマ	テーマ
効果的な標的型攻撃メール訓練について	脅威インテリジェンス活用によるセキュリティ強化の取り組み
クラウドサービス導入審査	自社の生成AI活用体制とそのセキュリティ審査について
セキュリティガバナンスの実行力向上のための技術的な取り組み	外部SOCの利用と、自社SIEM監視の各々の活用について
ゼロトラストセキュリティ環境の構成と課題	クラウド基盤のセキュリティ強化（CNAPP導入）について
ユーザー利用アプリ運用・管理	企業内のセキュリティガバナンス定着に向けた工夫（複数のセキュリティガバナンス規定の狭間で、、）
クラウドサービス利用管理と監査効率化の検討	サプライチェーンセキュリティ
インフラ部門が進めるログ監視運用の現状と課題	AIに関するセキュリティについて
特権ID管理の検討状況と悩み	セキュリティ運用管理の現状と課題について

2.4 分科会Bで扱ったテーマ

テーマ	テーマ
標的型メール訓練の運用について	取引先を狙った攻撃への対策
サイバーセキュリティ監査の初手	セキュリティ事故の経緯と対応　セキュリティ管理・運用について考える
国内グループ会社 セキュリティ均質化、監査における課題	社内電話帳の見直し
サイバー対処能力強化法：官民連携での資産登録	CSIRT発足当時と2年後の現状の状況
インターネット公開資産の管理	セキュリティ対応組織の教科書 Touch & Try
グループ各社のガバナンス強化について	EDR製品の導入と運用における課題
外部公開システム運用における課題	資産管理、脆弱性管理、対応範囲の実態について
セキュリティインシデント対応体制に関する悩み	外部サービス利用（SaaS, PaaS, IaaS, AI）管理の取り組み検討について

2.5 分科会Cで扱ったテーマ

テーマ	テーマ
セキュリティ人材育成	インシデント発生時の対応マニュアルについて
グループ全体のセキュリティ意識向上の必要性　～ セキュリティ体制強化に向けた今後の展望 ～	スタートアップフェーズでの取り組み
クラウドサービスの利用審査と利用管理について	全社的なサイバーセキュリティ訓練について
実行性あるIT-BCP	クラウドシステム利用のガバナンスについて
アクセス権管理ポリシと運用	情報セキュリティ監査の現状
全社情報セキュリティアウェアネス	システムリスクRCSAの点検項目
セキュリティインシデント事例とその対策/再発防止策について	国内外グループ会社における情報セキュリティ対策
M365のセキュリティ運用について	東日本大震災から15年、もう一度振り返ろう
グループのグローバルセキュリティ体制の構築について	

2.6 合宿でのインシデントゲームによる演習

● 演習の概要

仮想インシデント対応を題材としたゲーム形式の演習

・不確実な情報下での意思決定・初動判断を体験
・組織間の調整やコミュニケーションを実践
・合宿形式により、密度の高い議論を実現

● 主な気づき

意思決定と組織間連携が対応の成否を左右する

● その他の気づき

・判断基準や役割分担の事前整理が重要
・組織間の連携不足が対応の遅延や混乱を招く
・平時からの関係構築が円滑な対応に直結する
・インシデント対応は組織全体の運用として設計する必要がある

2.7 企業（セキュリティ統括組織および運用拠点）の見学

全体会でのゲスト講演の企業のご厚意により、研究会メンバーの有志９名でセキュリティを統括する組織の居室・設備を見学

・SOC等の設備および運用状況を確認
・教育・ガバナンス・可視化の取組みを共有
・参加者との意見交換を実施

● 主な気づき

統括組織の設計と運用の具体像を把握

● その他の気づき

・可視化と標準化が運用効率の向上に寄与している
・教育・訓練がセキュリティ水準の底上げに有効
・ガバナンスと現場運用のバランスが重要
・組織横断での情報共有と連携の仕組みが不可欠

第3章
分科会と実践で共有された課題

本研究会では、業種や立場の異なる参加者の議論を通じて、個別事象ではなく共通して発生している課題が整理された。
本章では、これらを「技術対策」「セキュリティ運用」「組織・ガバナンス」の3つの観点から整理する。

3.1 分科会の議論から見えてきた「成立しない現実」

- 現状

・技術は導入されている
・運用も回している
・ルールも存在している。

それでも

- 現実

現場では機能しない

3.2 技術対策をめぐる課題

技術対策は「導入」から**「扱えるかどうか」**の問題に変わっている

議論のエッセンス

EDR	ASM	ログ監視	クラウド
・アラート多すぎ ・判断できない	・資産は見えた ・多すぎて無理	・何を見るか不明 ・ログ多すぎ	・前提バラバラ
↓	↓	↓	↓
見ない前提	優先順位つけられない	使えていない	統一できない

見える化・高度化が進むほど、技術対策は「扱えない」状態に陥っている

3.3 セキュリティ運用をめぐる課題

セキュリティ運用は「回しているだけ」になっている

議論のエッセンス

アラート対応	監視体制	脆弱性管理	外部委託
・判断が人による ・担当者依存	・24/365は理想 ・実態は維持できない	・情報が多すぎる ・全部は無理	・委託しても最後は自社 ・丸投げすると不明化
↓	↓	↓	↓
再現性がない	見れられていない時間がある	選べない	依存もできない

やるべきことが増え続け、セキュリティ運用は「回らない」状態に陥っている

3.4 組織・ガバナンスをめぐる課題

セキュリティは「組織として実行できない」状態にある

議論のエッセンス

部門間の関係	グループ統制	ルールと統制	人材
・セキュリティ部門は調整役 ・主導できない	・会社ごとにバラバラ ・統一できない	・ルールはある ・守られない	・人がいない ・育たない
↓	↓	↓	↓
動かせない	レベル差が放置	選べない	回らない

役割・責任・人材が噛み合わず、セキュリティは組織として「動かない」状態に陥っている

3.5 実践から裏付けられた課題

分科会での議論は、実務の現場でも同様に発生している

インシデントゲーム			企業見学		
初動判断ができない	→	情報が不完全	対策が仕組みとして設計されている	→	個別対策ではない
意思決定が遅れる	→	判断基準が曖昧	教育・統制・可視化が一体的に運用	→	「回る仕組み」として統制
役割が曖昧	→	指揮が定まらない	組織全体での統制	→	バラつきを抑制
組織調整に時間がかかる	→	技術より調整がボトルネック	実務に組み込まれている	→	特別対応になっていない

課題の本質は、技術ではなく「組織として回らないこと」にある

第4章
セキュリティ対策を「成立させる」ための視点

第3章で整理した課題は、個別の対策不足ではなく、技術・運用・組織の構造に起因するものである。
そのため、単に対策を追加するのではなく、「成立する前提」で再設計することが必要である。
本章では、セキュリティ対策を企業の実務として成立させるための基本的な視点を整理する。

4.1 技術対策

技術対策は、「網羅」ではなく、「扱い続けられること」を前提に設計する必要がある

対策を絞る	優先順位を明確化	運用前提で設計	ツールの位置づけ
守る範囲を定義	重要度で判断	運用可能範囲に限定	ツールは手段
↓	↓	↓	↓
全てを対象にしない	迷いを減らす	継続可能にする	導入が目的にならない

扱い続けられない対策は、
結果として機能しない

4.2 セキュリティ運用

セキュリティ運用は「すべて対応する」のではなく、「回り続ける状態」を優先することが重要である

対応範囲を制御	判断基準を定義	役割分担を定義	外部活用を前提化
対象を絞る	ルールを明確化	責任を明確にする	委託範囲を定義
↓	↓	↓	↓
やらないことを決める	属人性を抑える	運用を安定させる	丸投げしない

継続的に実行できない運用は、それ自体がリスクとなる

4.3 組織・ガバナンス

セキュリティは「ルール」ではなく、「組織として動く形」で設計していく必要がある

構造と責任を明確化	統制の現実化	現場との整合	人材前提の見直し
実行主体を明確にする	実行可能な水準に調整	現場負担を考慮	体制で補う
↓	↓	↓	↓
動ける状態にする	形骸化を防ぐ	守れるルールにする	個人依存を減らす

組織として動き続ける状態を前提に、
対策を構造として捉える必要がある

第5章
本研究会を通じて見えた本質

本研究会で扱ったのは、個別の対策や技術ではない。

分科会での議論、インシデント演習、企業見学といった実践を通じて、企業のセキュリティ対策が現場でなぜ機能しないのか、その背景にある構造と向き合ってきた。

本章では、その過程で見えてきた本質的な論点を整理する。

5.1 実務の現場から見えた「三つの構造的課題」

セキュリティ課題は、個別の対策不足ではなく「構造」として発生している

単なる対策不足ではなく、良かれと思って導入した仕組みが、かえって運用の負荷を高めている実態が浮き彫りとなった。

ツール導入が目的化し、現場における判断軸が失われている

検知能力の向上により情報は増加しているが、何を優先し、何を捨てるかの判断が曖昧なままでは、実効性は確保されない。

「検知」と「対応」の間に構造的な断絶が存在する。

異常を検知する仕組みは整備されつつある一方で、それを受けて動く人員や意思決定の仕組みが追いつかず、結果として対応が回らない。

ルールと現場の乖離である。

統制強化のために設けられたルールが現場の実態と乖離し、形骸化する一方で、現場では独自の判断が進むという分断が生じている。

5.2 対話で直面した「相反する価値の最適化」

セキュリティは、相反する価値の中で成立させる必要がある

「対策の高度化」と「運用の持続可能性」の乖離

技術の高度化を進めれば現場の運用負荷は増大し、運用の持続可能性との間に乖離が生じる。最新よりも自社の身の丈に合った長く回し続けられる仕組みを求める声。

「統制の強化」と「現場の機動力」の摩擦

統制を強化すれば現場の機動力は低下し、逆に現場の裁量を広げれば統制の一貫性は損なわれる。セキュリティ側の「正しさ」を押し付けるのではなく、ビジネスのスピードとどう折り合いをつけるか

「中央による統治」と「分散組織の裁量」の折り合い

グループ全体での統一を図る中央的な統制と、各拠点・各社の実情に応じた分散的な判断との間にも、常に調整が求められる。

5.3 実践を通じて確認されたこと

セキュリティの成否は、技術ではなく「組織の意思決定と動き方」によって決まる

インシデント演習で見えたこと

不完全な情報のもとで、判断・連携・調整が想像以上に難しい
初動の遅れや判断の迷いが、そのまま被害拡大につながる構造が確認された

対応を止める本当の要因

技術不足よりも、「誰が判断するか」「何を基準に決めるか」の曖昧さ
役割や責任が不明確なままでは、情報があっても意思決定が進まない

企業見学で確認されたこと

教育・統制・可視化が一体化した、継続的に回る仕組みが重要
特定の担当者に依存せず、組織として回る設計が実効性を左右する

5.4 経営視点への昇華

セキュリティは「技術課題」ではなく「経営課題」である

投資の見方を変える

導入費だけでなく、人材育成・訓練・調整まで含めて評価する
短期的なコストではなく、継続的に統制を維持するための投資として捉える必要がある

守る範囲は経営が決める

「どこまで守るか」「どこから受け入れるか」は現場任せにしない
リスク許容の水準を明確にしない限り、現場の判断は分断され一貫性を失う

担当者の役割は橋渡し

経営と現場の間に立ち、優先順位の合意形成を進める
技術的な正しさだけでなく、事業とのバランスを踏まえた意思決定を支えることが求められる

5.5 対話の本質と研究会の意義

本研究会の価値は、「答え」ではなく「問い」を共有したことにある

他社事例は「正解」ではない

本研究会では、他社の取組みをそのまま適用するのではなく、自社の前提を見直す材料として捉えた
結果として、自社の体制や判断基準を相対的に捉える視点が共有された

対話によってズレが見えた

分科会や全体会での議論を通じて、立場や企業ごとの優先順位の違いが明確になった
特に、現場と経営、技術と統制の間にある認識のズレが具体的な形で可視化された

対話が理解を深めた

企業や立場の異なる参加者同士の議論により、単独では得られない多面的な気づきが得られた
組織内では見えにくい課題や前提が整理され、議論の質が高まった

5.6 対話から得た確信を次の一歩へ

本研究会を通じて得られた気づきを踏まえ、各企業が次の一歩として取り組むべき方向性を整理する。

セキュリティは「技術だけでは成立しない」

本研究会を通じて、対策の成否は組織・意思決定・運用の設計に大きく依存することが確認された
各社においても、技術導入だけでなく「どう運用し、どう判断するか」を改めて見直す必要がある

対話が「前提」を揺さぶった

企業や立場の違いを越えた対話により、自社の常識や前提を相対化する機会が得られた
その気づきを持ち帰り、自社の前提や判断基準を問い直すことが出発点となる

次の一歩は「各社での実践」にある

本研究会は答えを提示する場ではなく、問いと視点を持ち帰る場であった
ここで得た問いをもとに、各社の状況に応じた具体的な改善と実践につなげていくことが重要である

本研究会を通じて

各分科会において議論の整理・取りまとめにご尽力いただいた分科会長・副分科会長の皆様、本研究会の運営に携わっていただいた副部会長をはじめとする幹事団の皆様、活動を支えていただいたJUAS関係者の皆様、ならびに本研究会の活動に多くの示唆と機会を与えていただいた関係者の皆様、

そして発表準備および議論を通じて知見を共有いただいたすべての参加者の皆様に、深く感謝の意を表する。

今後もそれぞれの現場において、

活かされていくことを期待する。

付録 本研究会へのご参加企業一覧（1/2）五十音順

本研究会は、多様な業種の企業における実務担当者の参加により構成されていた。

組織名	業種	組織名	業種
株式会社IHI	製造	株式会社オカムラ	製造
イオン株式会社	小売／流通	オリックス・システム株式会社	金融・情シス子会社
株式会社インターネットイニシアティブ	ITサービス	かんぽシステムソリューションズ株式会社	金融・情シス子会社
インフォテック株式会社	ITサービス	株式会社かんぽ生命保険	金融
株式会社ウテナ	製造	コープ情報システム株式会社	生協・情シス子会社
株式会社エイジス	その他	サイバネットシステム株式会社	ITサービス
エクシオグループ株式会社	ITサービス	JFEシステムズ株式会社	製造・情シス子会社
エス・エー・エス株式会社	ITサービス	JFEスチール株式会社	製造
ＮＲＩシステムテクノ株式会社	ITサービス	JALデジタル株式会社	交通・情シス子会社
ＮＯＫ株式会社	製造	独立行政法人住宅金融支援機構	金融
株式会社NTTデータMHIシステムズ	製造・情シス子会社	新電元工業株式会社	製造
ENEOSホールディングス株式会社	エネルギー	双日テックイノベーション株式会社	ITサービス

付録 本研究会へのご参加企業一覧（2/2） 五十音順

組織名	業種	組織名	業種
ＳＯＭＰＯひまわり生命保険株式会社	金融	株式会社ニッスイ	食品
株式会社大同ＩＴソリューションズ	製造・情シス子会社	日本航空株式会社	交通
株式会社中電シーティーアイ	エネルギー・情シス子会社	日本ハム株式会社	食品
DIC株式会社	製造	パーソルキャリア株式会社	人材サービス
帝人株式会社	製造	東日本旅客鉄道株式会社	交通
株式会社テプコシステムズ	エネルギー・情シス子会社	日立建機株式会社	製造
電源開発株式会社	エネルギー	ファイルフォース株式会社	ITサービス
東京海上日動システムズ株式会社	金融・情シス子会社	株式会社富士薬品	製造
東邦ガス株式会社	エネルギー	株式会社ブリスコラ	ITサービス
株式会社TRAILBLAZER	ITサービス	丸文株式会社	商社
株式会社ニチレイ	食品	森永乳業株式会社	食品
日揮コーポレートソリューションズ株式会社	総合エンジニアリング・情シス子会社	株式会社レゾナック・ホールディングス	製造
日揮ホールディングス株式会社	総合エンジニアリング		