HITACHI
Inspire the Next

重要インフラのセキュリティとその共通課題

日立製作所セキュリティトラスト研究部　河内　尚

自己紹介

電気学会C部門に所属
　活動分野：サイバーセキュリティ
　　・2024年　技術調査委員会「重要インフラセキュリティ」の委員長を拝命

研究分野 （自動車、鉄道、金融、医療、情報通信のセキュリティ）

車車間通信システムの研究開発

車車間無線通信セキュリティチップおよび暗号ソフトウェア	2007-2010
車車間通信鍵管理システムのセキュリティ機能設計	2017
車載情報機器のセキュリティ脅威分析および運用管理ポリシー策定	2014

セキュリティ設計・脆弱性管理技術の研究開発

車載通信システムのセキュリティ設計、セキュリティ管理体制構築	2017-2020
鉄道IoTシステムのセキュリティ設計、脆弱性試験手法	2021-2023
DevSecOps開発手法	2023-2024

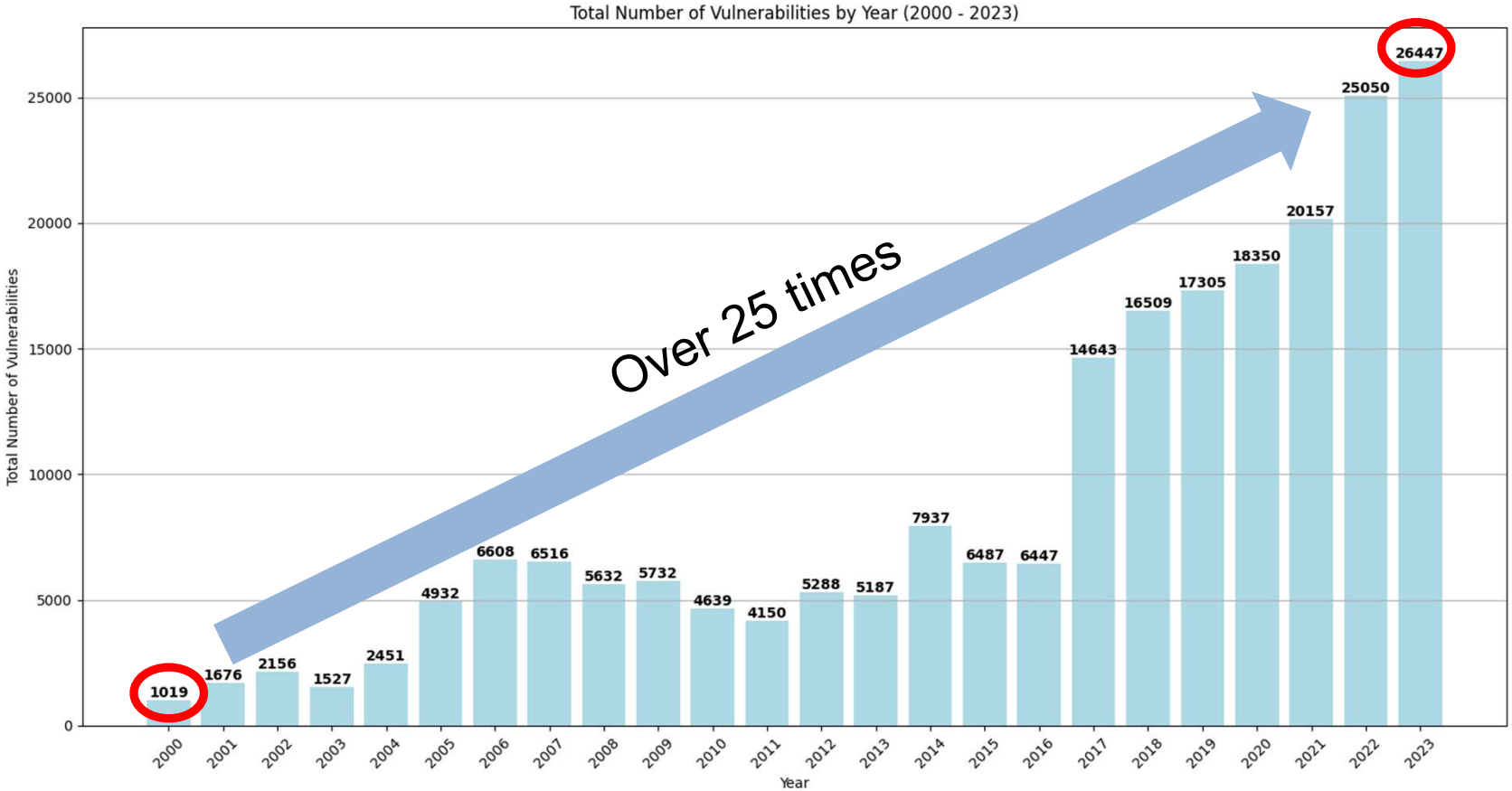
HITACHI
Inspire the Next

1. 背景
2. 日米欧亜のセキュリティ要件比較
3. 結言

1. 公開された脆弱性の傾向

HITACHI
Inspire the Next

重要インフラの開発においてもOSS等の汎用技術の利用が増加、公開される脆弱性は激増
脆弱性公開からパッチ適用前に攻撃される事例も増加



Source : https://blog.qualys.com/vulnerabilities-threat-research/2023/12/19/2023-threat-landscape-year-in-review-part-one

HITACHI
Inspire the Next

1. 背景
2. 日米欧亜のセキュリティ要件比較
3. 結言

JP

2-1. 重要インフラのサイバーセキュリティに係る行動計画

日本においては、NISC(サイバーセキュリティ戦略本部)により「重要インフラのサイバーセキュリティに係る行動計画」が策定されており、この計画では15の重要分野が指定。具体的には、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流、化学、クレジット、石油、港湾がこれに該当。

目的：重要インフラにおいて、任務保証の考え方を踏まえ、安全かつ持続的な提供を実現
- 重要インフラサービスの継続提供を不確かなものとするリスクを許容範囲に抑制する
- 重要インフラサービス障害に備えた体制を整備する
- 障害は発生時に適切な対応を行い、迅速な復旧を図る

方向性：行動計画に基づいて以下施策と補強・改善の方向性が示されている。
1. 障害対応体制の強化
2. 安全基準等の整備及び浸透
3. 情報共有体制の強化
4. リスクマネジメントの活用
5. 防護基盤の強化

(NISC)重要インフラのサイバーセキュリティに係る行動計画
https://www.nisc.go.jp/policy/group/infra/siryou/index.html

US

2-2. 大統領令Executive Order 14028(EO-14028)

HITACHI
Inspire the Next

米国政府とインフラの安全確保のための基本的な方向性(2021年)

#	カテゴリ	内容
1	脅威情報の共有に対する障壁の除去	サービスプロバイダーに対し、政府のネットワークに影響を与える可能性のあるサイバーインシデントや脅威情報を共有することを義務付ける
2	連邦政府のサイバーセキュリティのモダナイゼーション	連邦政府は、クラウド サービス、ゼロトラスト アーキテクチャ、多要素認証と暗号化の導入を保護します。
3	ソフトウェアサプライチェーンのセキュリティの強化	政府に販売されるソフトウェアの開発に関するベースラインセキュリティ基準を確立し、開発者にソフトウェアの可視性を高めることを義務付ける(SBOM(Software Bill of Materials))
4	サイバー安全審査委員会の設置	重大なサイバーインシデント後に招集され、何が起こったのかを分析し、勧告を行う可能性のあるサイバーセキュリティ安全審査委員会を設立します。
5	サイバーセキュリティの脆弱性とインシデントに対応するための連邦政府のプレイブックの標準化	連邦政府の省庁によるサイバーインシデント対応のための標準化されたプレイブックと一連の定義を作成します
6	連邦政府のネットワークにおけるサイバーセキュリティの脆弱性とインシデントの検出の改善	政府全体のエンドポイント検知・対応システム(脆弱性検知、セキュリティテスト)の実現により、連邦ネットワーク上の悪意のあるサイバー活動の検知能力の向上
7	連邦政府の調査および修復能力の向上	連邦政府機関向けのサイバーセキュリティイベントログ要件を作成し、侵入を検知する組織の能力を向上させます。

US

2-3. CIRCIA(重要インフラのサイバーインシデントレポート. Act)

HITACHI
Inspire the Next

重要なインフラにおけるインシデント報告の規制。(2022年)。発効日は25年度

#	必要条件	内容
1	対象となるサイバーインシデントレポート	対象サイバーインシデントを経験した対象事業体は、対象事業体がインシデントが発生してから72時間以内にCISAに報告しなければなりません
2	Ransom Payment Reporting	ランサムウェア攻撃の結果として身代金の支払いを行う、または別の事業体に身代わりの支払いを依頼する対象事業体は、支払いが支払われてから 24 時間以内に CISA に報告する必要があります
3	Supplemental Reporting	対象事業体は、次の2つの状況において、速やかにCISAに補足報告書を提出する必要があります。 - 以前に新規脆弱性の情報を対象としたサイバーインシデント - 事業体、またはその代理となる別の事業体が身代金の支払いを行う （カバードサイバーインシデントに関連）
4	データと記録の保存	CIRCIAレポートの提出が義務付けられている対象事業体は、特定のデータと記録を保存する義務があります

US

2-4. FD&C(食品、医薬品、化粧品) Act

HITACHI
Inspire the Next

医療機器については、大統領令に対応してサイバーセキュリティ要件が追加

Section	#	サイバーセキュリティ要件
524B	1	調整された脆弱性の開示および関連手順を含む、市販後のサイバーセキュリティの脆弱性およびエクスプロイトを監視、特定、および必要に応じて合理的な時間内に対処するためのを長官に提出します
	2	デバイスおよび関連システムがサイバーセキュリティであることを合理的に保証するためのプロセスと手順を設計、開発、および維持し、デバイスおよび関連システムに対する市販後のアップデートおよびパッチを利用可能にして、以下に対処するため。 (A) 合理的に正当化された定期的なサイクルで、既知の許容できない脆弱性。そして (B) 制御不能なリスクを引き起こす可能性のある重大な脆弱性をできるだけ早くサイクルから外します
	3	商用、オープンソース、および既製のソフトウェアコンポーネントを含むソフトウェア部品表(SBOM)の提供する
	4	長官が規制を通じて要求するその他の要件を遵守し、デバイスおよび関連システムがサイバーセキュアであるという合理的な保証を実証します

EU

2-5. EU cybersecurity regulations

HITACHI
Inspire the Next

NIS2 Directive and CRA は厳しい基準と要件を策定し 進化するサイバー脅威からデジタルインフラストラクチャと製品を保護することを要求

	NIS2(Network and Information Security) Directive	Cyber Resilience Act (CRA)
Purpose	EU全体のサイバーセキュリティを強化。	デジタル要素を備えた製品が厳しいサイバーセキュリティ基準を満たしていることを確認。
Scope	ヘルスケア、エネルギー、運輸、銀行、デジタルインフラなどの幅広い分野。	ネットワークに接続されているソフトウェアとハードウェアに適用。(例:産業用ファイアウォール、産業用ルーター、スマートメーターなど)
Security Measures	リスク評価、インシデント対応計画、サプライチェーンセキュリティ、セキュリティテスト。	Security Design、脆弱性管理、リスク評価、インシデント管理、透明性、ライフサイクルサポート、SBOM、定期的かつ効果的なセキュリティテスト。
Reporting Obligation	最初のレポート:24時間以内、更新:72時間以内、最終レポート:1か月以内。	最初のレポート:24時間以内、更新:72時間以内、最終レポート:1か月以内。
Timeline	2024 年 10 月 17 日までに国内法に適用。	2024年後半に発効し、2027年までに遵守。

ASIA

2-6. アジア規制(インド、マレーシア、シンガポール、インドネシア)

HITACHI
Inspire the Next

各地域の規制によりコンプライアンス対応とセクター認証のコストが増加している

Finance	Critical Infrastructure	Digital
RBI, SEBI mandated updated supply chain security requirements	CEA guidelines mandate sourcing from “Trusted sources”	Regional Data protection, privacy regulations with stringent penalties

[India] RBI’24 : Security Testing Mandatory from Apr’25

PSOは、すべてのアプリケーションが、認証モードで資格のある専門家を通じて適切な頻度(少なくとも年次ベース)で、ソースコードレビュー、VA、PTなどの厳格なセキュリティテストを受けることを保証するものとします。
最初の報告 – 検出から6時間以内
[インド]SEBI'24: SBOM は 4 月 25 日から義務化されます
規制対象事業体は、コードベースで使用されるすべてのオープンソースおよびサードパーティのコンポーネントを含む新製品を調達する前に、新製品のSBOMを取得するものとします。
最初の報告 – 6 時間以内、最終報告 – 14 日以内

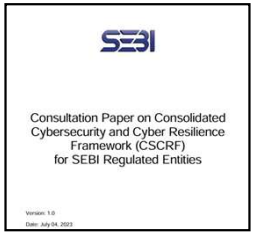
[India] CEA’21 : Mandatory Product Security Testing from ‘22

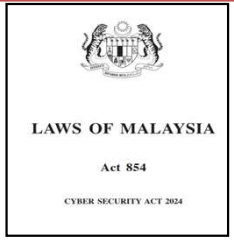
インフラストラクチャ/システムに必須に導入されたすべての ICT ベースの機器/システムは、CEA によって作成された「信頼できる情報源」のリストから調達されます
最初の報告 – 発生から 24 時間以内

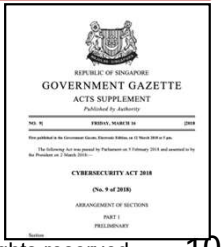
[Malaysia, Singapore] Laws for Data and Critical Infra’24:

- 個人データの外部転送は、PDPA第129条(3)に規定されている条件に準拠する必要があります。
- サイバーセキュリティのラベリングスキームでは、ヘルスケアのような重要な分野でバイナリ分析とペネトレーションテストが義務付けられている。

India – RBI Guidelines for Payment Security’24	India – SEBI Cybersecurity Framework’ 24	India – DPDA’23	India – CEA Guidelines’ 21	Malaysia – Cybersecurity Law’24	Indonesia - PDP’22	Singapore – Cybersecurity Act’24







RBI: Reserve Bank of India. SEBI : Securities Exchange Board of India. CEA: Central Electricity Authority

2-7.セキュリティ共通要件

HITACHI
Inspire the Next

セキュリティ設計、構成管理、セキュリティテスト、脆弱性管理、インシデント報告/対応と修復は、主要要件である

#	Common requirements	JP	US	EU	ASIA(India etc.)
1	セキュリティ設計	○	○	○	○
2	ソフトウェア構成管理	SBOM	SBOM	SBOM	SBOM
3	セキュリティテスト	望ましい	Detection of vulnerabilities	Regular and effective testing	Binary analysis/ penetration testing
4	脆弱性管理	規程有	Mandatory	Mandatory	Mandatory
5	インシデント報告義務	規程有	72hours	24hours 72hours 30days	6hours 24hours
6	インシデント対応と修復	規程有	Standard playbook	Making BCP	Immediate response (7days-14days)

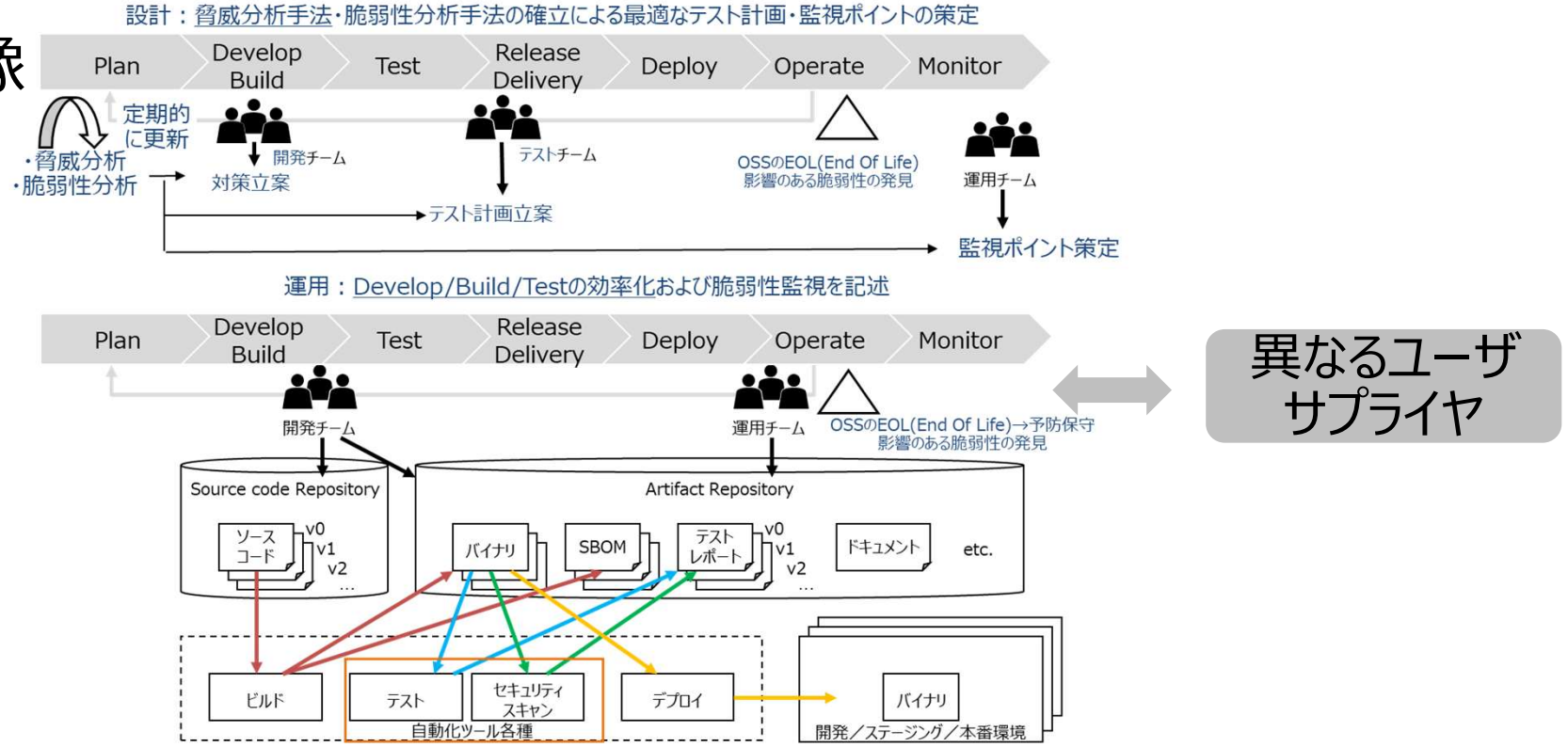
HITACHI
Inspire the Next

1. 背景
2. 日米欧亜のセキュリティ要件比較
3. **結言**

考察(私が課題だと思う事)

セキュリティ要件に対応しようとすると、即応体制、社内外の連携、教育および技術研究開発が課題
社内：各部署との連携、セキュリティ人材の育成、社内プロセスの整備、
運用管理手法、SBOMを活用した脆弱性検知/対応、脆弱性試験等の関連技術開発
サプライチェーン：異なるユーザ、サプライヤーの協働によるサイバーセキュリティの確保、迅速な対応の構築

理想像



期待　その１　「インフラストラクチャーのためのサイバーセキュリティ対策」

HITACHI
Inspire the Next

セキュリティ要件に対応しようとすると、以下が体制、社内外の連携、教育および技術研究開発が課題
　社内：各部署との連携、セキュリティ人材の育成、社内プロセスの整備、
　　運用管理手法、SBOMを活用した脆弱性検知、脆弱性試験等の関連技術開発
　サプライチェーン：異なるユーザ、サプライヤーの協働によるサイバーセキュリティの確保、迅速な対応の構築

幅広い分野の知見に基づく研究発表

①【総論】「重要インフラのセキュリティとその共通課題」
講演者：河内　尚（日立製作所）
②【産業制御系】「産業制御システムに求められるサイバーセキュリティ対策」
講演者：出口　博一様（MOXA Japan合同会社）
③【電力】「電力事業者におけるサイバーセキュリティ対策と運用の実態」
講演者：長谷川弘幸様（中部電力株式会社　DX推進部エキスパートセキュリティセンター
④【鉄道】「鉄道インフラのサイバー脅威と対策の現状」
講演者：川﨑　邦弘様（公益財団法人　鉄道総合技術研究所　研究開発推進部）
⑤【通信】「通信インフラのサイバーセキュリティ対策」
講演者：林　正博先生（東京都市大学　理工学部　電気電子通信工学科）
⑥【教育・人材育成】「教育現場におけるインフラセキュリティ人材の育成」
講演者：城間　敏生先生（前沖縄県立浦添高校　校長）

期待　その２　B部門とC部門の重要インフラセキュリティ分野での緊密な連携への期待

HITACHI
Inspire the Next

・重要インフラセキュリティの研究開発分野は今後ますます重要となる
（電気学会の強み：制御システムの知見とサイバーセキュリティの知見の組み合わせ）
・制御システムを含むインフラセキュリティは学際領域であり、システム要件、適応事例、サプライチェーン管理等でB部門との意見交換、情報共有等、これまで以上の緊密な連携を期待

TC14　重要インフラのセキュリティ

（技術委員会提案企画セッション）

オーガナイザ・座長：河内　尚（日立製作所）
座長：中谷 博司（東芝）

現在，重要インフラを取り巻くセキュリティ環境は，IoT（Internet of Things）やAI（Artificial Intelligence）技術の進展に伴い急速に変化している。このような課題に対応し分野横断型新システム創成技術委員会では、重要インフラのセキュリティ調査専門委員会を2024年11月に発足させた。本セッションでは、同委員会による（1）重要インフラのセキュリティに関する課題，攻撃事例，技術動向（2）エネルギー分野を始めとする法規制やガイドライン，対策プロセス動向、（3）IoTやAI技術のセキュリティに与える影響および同技術の利活用によるセキュリティ対策強化に関する調査内容を紹介する。

TC14-1　電力・エネルギー部門におけるサイバーセキュリティ関連の活動状況と今後への期待※原稿投稿なしの講演 …… 大谷哲夫（電力中央研究所）

TC14-2　IEC 61850 ユニキャスト通信における IEC 62351 に基づくセキュリティ共通仕様の提案 …… ○嶋田丈裕，上田紀行，平川哲也（電力中央研究所） …… 559

TC14-3　重要インフラ事業における PSIRT 活動 …… ○天木　智（東芝） …… 561

TC14-4　重要インフラの機能安全とセキュリティ …… ○中谷博司（東芝） …… 565

TC14-5　実験データの時間シフトを用いた VIMT を狙った毒化攻撃に対する防御法の検討 …… ○池崎太一（岡山大学），澤田賢治（大阪大学），金子　修（電気通信大学） …… 568

TC14-6　電力分野におけるサイバーセキュリティに関する法規制やガイドライン …… ○千賀　章（東京電力パワーグリッド） …… 573

TC14-7　AI 特有の脅威の概要とリスク評価への取り組み …… ◎小松みさき，花谷嘉一（東芝） …… 576

TC14-8　鉄道システム向け脆弱性分析手法 …… ○ Takashi Kawauchi（日立製作所） …… 581

TC14-9　制御システムの状態遷移系列に基づく脆弱性評価と構造的リスク解析 …… ◎岡村望夢（電気通信大学），澤田賢治（大阪大学），久野倫義，宮内茂人（三菱電機） …… 583

B部門特別講演

8/29 C部門大会でのB部門とC部門の
「重要インフラのセキュリティ」連携セッションの取り組み