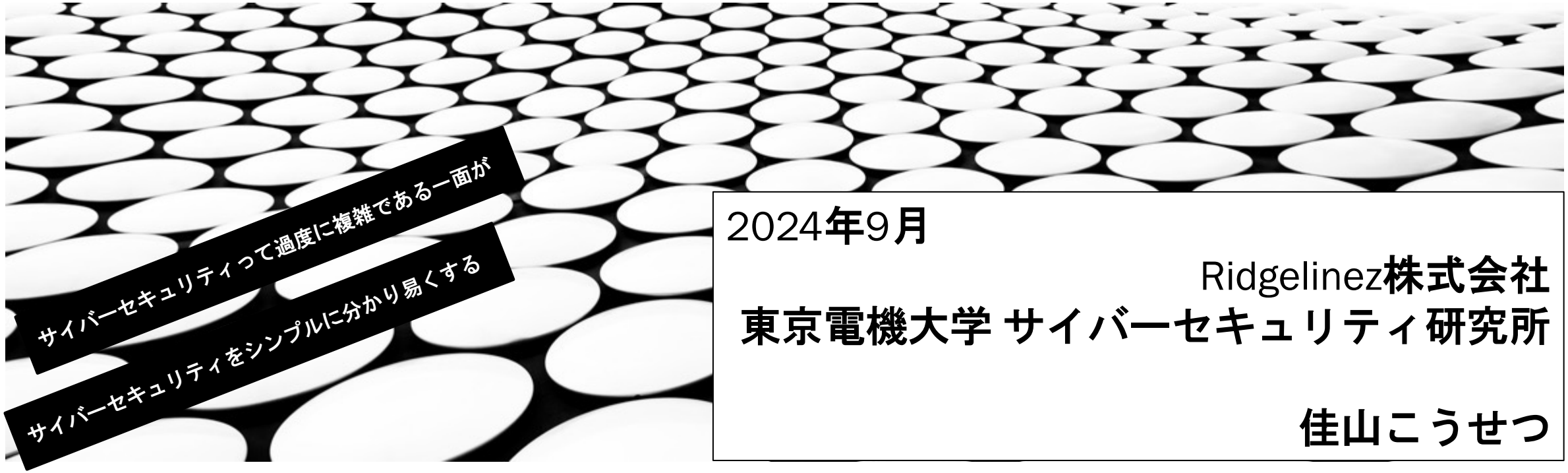
FISAC金融部会 勉強会

動きの読みづらいサイバーセキュリティの勘所

～いま何が起きているのか公開事例から読み解く～



2024年9月

Ridgelinez株式会社
東京電機大学 サイバーセキュリティ研究所

佳山こうせつ

佳山 こうせつ（かやま こうせつ）

2004年 **個人情報保護法 → ルールの制定、プロセス違反に対する厳しい罰則**

2007年 セキュリティ業界コミュニティへ参画

2010年 内閣官房情報セキュリティセンター委員 [退任]
情報処理推進機構(IPA)委員

2014年 **ソニーハック、Shellshock → 高度な技術の攻防**

2015年 ハッカーコミュニティSECCON実行委員[退任]
東京電機大学サイバーセキュリティ研究所研究員
セキュリティキャンプ顧問(キャンプ協議会)

2017年 **SecHack365トレーナー(総務省、NICT)**
中央大学、名古屋工業大学、など社外講師
IPA情報処理安全確保支援士 カリキュラム委員
国土交通省最高情報セキュリティアドバイザー[退任]

2024年 **？？？？？？？**

セキュリティ設計したシステムが攻撃被害

①攻撃手法の探求

自分らだけがセキュリティできてもだめ

②サイバーセキュリティに触れる場作り

社会問題に根深くささるサイバー攻撃

③サイバーを通して社会変化を見て発信

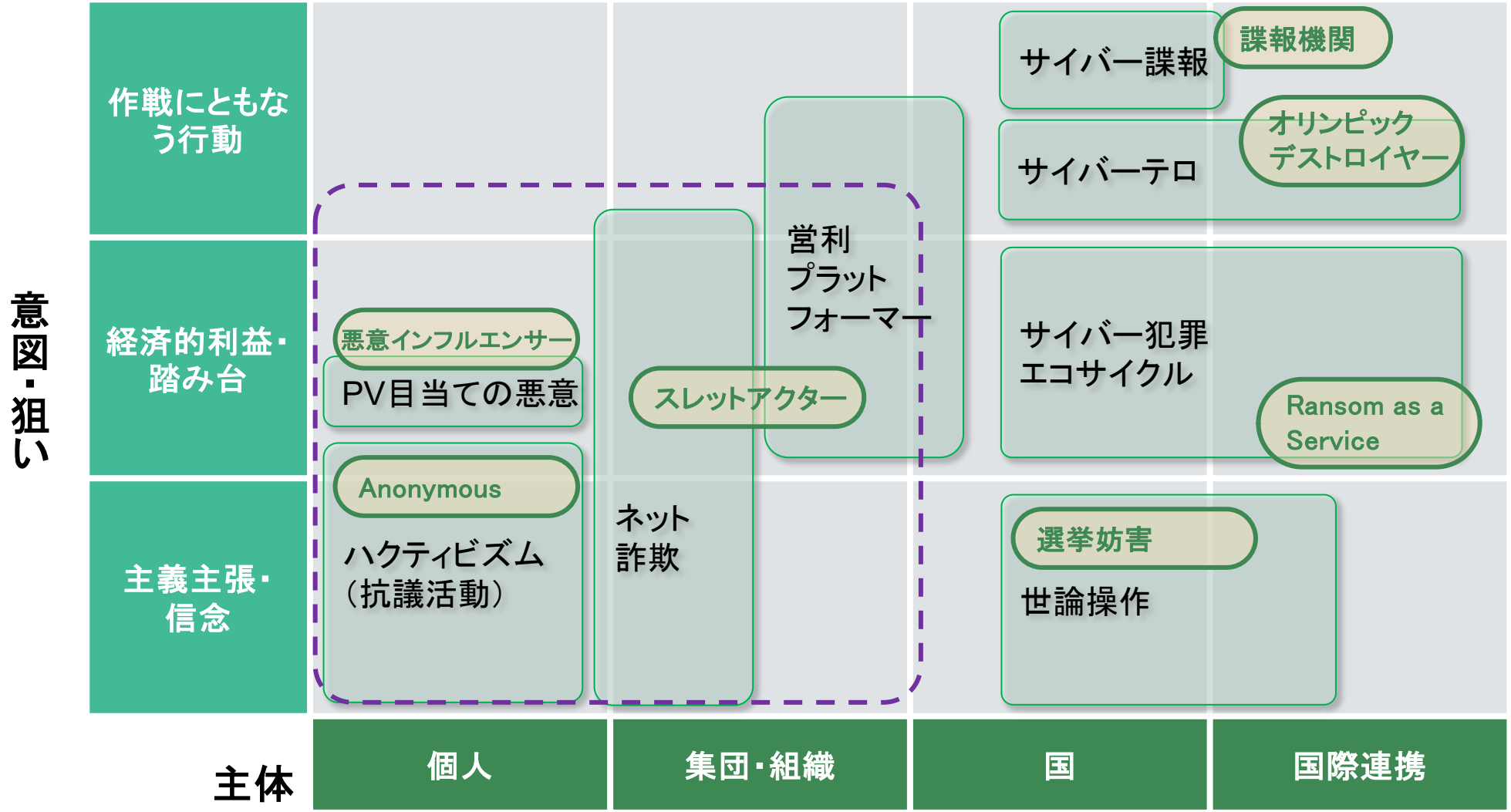
本セッションのゴール設計

言葉じりだけ先行するサイバーセキュリティ
実際のところどうなの？ってのを考えるきっかけに

＋

基本的な対策(全体設計、構成管理、ログ管理など)が大切

サイバーセキュリティって、考えなきゃいけないことが広すぎる
ひも解くヒント①：目的/主体で整理



ひも解くヒント②：３つの視点

投影のみ

ひも解くヒント③：３つの視点

A 利用者の視点

B 産業界の視点

C 専門家の視点

目次

問いかけ ①

ネット使っていて、なにか怖い目にあったことがあったら共有ください。

差し支えない範囲で、チャットにてコメントください。

ひも解くヒント：３つの視点

A 利用者の視点

B 産業界の視点

C 専門家の視点

問いかけ②

最強のセキュリティとは？

差し支えない範囲で、チャットにてコメントください。

メッセージ：デジタル社会を支えるサイバーセキュリティ

守るセキュリティつなげるセキュリティへ。
どうやったら安心安全にデジタルデータをネットにつなげ活用できるか、セキュリティとともに考える。

問いかけ③

サイバーって何でしょうか？

差し支えない範囲で、チャットにてコメントください。

ひも解くヒント②：３つの視点

問い掛け④

どんなコンピュータがつながってます？

差し支えない範囲で、チャットにてコメントください。

デジタル社会という変化　～生活に密着するデジタル～

A 利用者の視点
B 産業界の視点
C 専門家の視点

- 昔の概念

- 近年の概念

Special Thanks：いらすとやさん
https://www.irasutoya.com/p/terms.html

デジタル社会という変化　～生活に密着するデジタル～

A 利用者の視点
B 産業界の視点
C 専門家の視点

- 昔の概念

- 近年の概念

問いかけ⑤

デジタル社会を感じるシーンはありますか？

差し支えない範囲で、チャットにてコメントください。

目次

事例１：狙われるVPN装置

どういうこと？

Cybersecurity Dive

Ivantiから2つのゼロデイ脆弱性に対するパッチがリリース 攻撃者の悪用進む

Ivanti Connect SecureとIvanti Policy Secureに深刻度の高い脆弱性が2件存在することが分かった。サイバー攻撃者はこれらのゼロデイ脆弱性をつなぎ合わせて、悪質なWebシェルで数千台のデバイスを侵害した。

2024年02月24日 07時00分 公開　[David Jones, Cybersecurity Dive]

印刷　通知　見る　Share　B!　0

PR 第5世代Xeon　AI推論パフォーマンスは"第3世代のなんと14倍"
PR 転職して1年あまり　30歳前後の若いエンジニアはどう変わった？

この記事は**会員限定**です。会員登録すると全てご覧いただけます。

ソフトウェア企業のIvantiは2023年12月上旬から、国家との関連が疑われる攻撃者によって悪用されていた「Ivanti Connect Secure」と「Ivanti Policy Secure VPN」における2つの脆弱（ぜいじゃく）性に対するセキュリティパッチをリリースした（注1）。

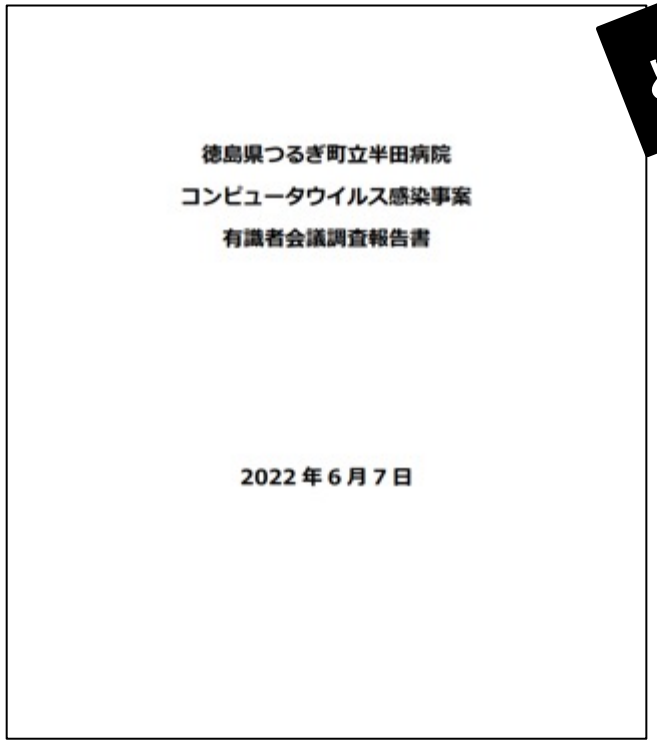
これらの脆弱性を悪用することで、数千台のIvantiデバイスが危険にさらされた。米国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）は連邦政府機関に対し、早急な対策を講じるよう緊急指令を出すに至った（注2）。

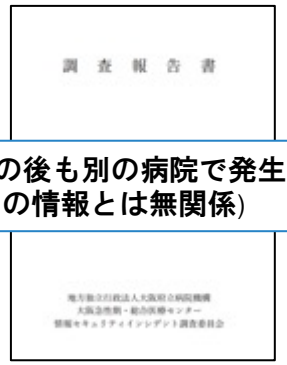
出典：https://www.itmedia.co.jp/enterprise/articles/2402/24/news013.html

投影のみ

事例２：被害にあった予算の限られた業種・業態

どういうこと？





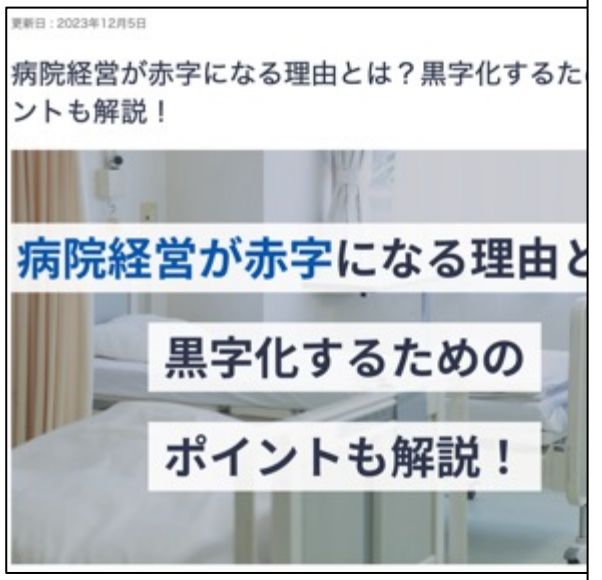
その後も別の病院で発生
(右の情報とは無関係)

出典：https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

出典：https://www.gh.opho.jp/pdf/report_v01.pdf (**右の情報とは無関係**)

投影のみ

事例２：被害にあった予算の限られた業種・業態



医療情報システム（IT）全体の費用合計額は年間1,800万～4,800万円/100床

次に医療情報システムですが、**費用合計額が民間病院で低く（年間約1,800万円）、国立病院で高い（年間約4,800万円）傾向**は医療機器と同様です。医療情報システムはMRIやCTなどの医療機器と異なり、稼働させても診療報酬で評価されないため、病院の収益向上には直結しません。そのため、**医療情報システムを導入・活用することによる効果を試算し、費用対効果を事前に検証することが重要になります。**

医療情報システム（IT）全体の100床あたり保守管理費用と構成割合

医療機器や医療情報システムの保守管理は費用内訳がブラックボックスで、詳細なベンチマークが難しい現状があります。コストマネジメントをするうえで、このような全国の平均値を参考にするのも有効な手段になるでしょう。

（出典：日本病院会「平成28年度医療機器・医療情報システム保守契約、費用に関する実態調査」）

出典：https://biz.moneyforward.com/establish/basic/52499/

出典：https://costsouken.jp/magazine/2355/

投影のみ

事例３：カジュアル管理者

どういうこと？

PDF Report at ZDNET

相次ぐ設定ミスによる情報漏えい--クラウドセキュリティのあるべき姿

PDF Report@ZDNET　2024-01-25 06:30

基幹を含めたシステムのクラウドシフトの大きな流れを背景に、クラウドセキュリティの重要性が年々増している状況だ。特に注目されているのが、設定ミスによる情報漏えいなどのセキュリティ事故である。

2023年5月には、トヨタ自動車が設定ミスによって顧客の車載端末IDや車体番号などの情報にアクセスし得る状況となってしまった。同年8月には、山口県の宇部市で「Teams」の設定ミスの原因により、小学校の児童の個人情報が漏えいする事故が起きた。

出典：https://japan.zdnet.com/article/35214320/

投影のみ

事例３：カジュアル管理者

どういうこと？

EV充電器、米ロでサイバー被害　安全保障リスクに

IoT　＋フォローする

2023年12月5日 2:00 [会員限定記事]

保存

Think!　多様な観点からニュースを考える　松原実穂子さんの投稿

電気自動車（EV）の充電器を狙うサイバー攻撃の脅威が増している。米国やロシアではハッキングにより画面が改ざんされ、英石油大手シェルは利用者情報の漏洩に見舞われた。専門家はEVが本格普及した際は安全保障上のリスクになりうると警鐘を鳴らす。

「これは私がやったんだ!」――。米エレクトリファイ・アメリカが中西部インディアナ州で運営する充電スタンドで撮影されたある画像がこの夏、インターネット上で話題を集...

出典：https://www.nikkei.com/article/DGXZQOUC175LD0X11C23A1000000/

投影のみ

事例まとめ：大切なのは基本、ただし欠如ではなく時代の変化

事象

- 狙われるVPN装置
- 業種の事情
- カジュアル管理者

届けたい盲点、事象の背景

- 基本的な役割分担が大切
- 基本的な運用設計、運用事項の洗い出し大切
- 基本的な設計が大切/基本リテラシー

ちなみに、外的要因はかなり進化しています。

投影のみ

ひも解くヒント②：３つの視点

投影のみ

ひも解くヒント②：３つの視点：某インシデントA[ご参考]

投影のみ

ひも解くヒント②：３つの視点：某インシデントB [ご参考]

投影のみ

目次

佳山 こうせつ（かやま こうせつ）

2004年 **個人情報保護法 → ルールの制定、プロセス違反に対する厳しい罰則**

2007年 セキュリティ業界コミュニティへ参画

2010年 内閣官房情報セキュリティセンター活動[退任]
情報処理推進機構(IPA)活動

2014年 ソニーハック、Shellshock → 高度な技術の攻防

2015年 ハッカーコミュニティSECCON実行委員[退任]
東京電機大学サイバーセキュリティ研究所研究員
セキュリティキャンプ(経産省、IPA)

2017年 SecHack365(総務省、NICT)
中央大学、名古屋工業大学、など社外講師
情報処理安全確保支援士更新教育 カリキュラム委員
国土交通省最高情報セキュリティアドバイザー[退任]

2024年 盲点が生まれるポテンヒット →時代の変化に”組織”と“ひと”が追随できず基本が置き去り

セキュリティ設計したシステムが攻撃被害

①攻撃手法の探求

自分らだけがセキュリティできてもだめ

②サイバーセキュリティに触れる場作り

社会問題に根深くささるサイバー攻撃

③サイバーを通して社会変化を見て発信

ひも解くヒント②：３つの視点

基本的なことが大切

- 脅威 x 脆弱性 x 資産価値 ＝ リスク
  - 脅威を知る。狙い所を知る。組織全体で知る。
  - 脆弱性を作らないアタックサーフェスマネージメント、パッチマネージメント
  - 構成管理とログ管理

→時代が変わっても基本は変わらないという勘所

問いかけ⑥

基本的な対策で大事にしていることは何ですか？

差し支えない範囲で、チャットにてコメントください。

知る。ポリシーベースだけではない、しっかり考えるセキュリティ

- システムに携わるひとは、その行間さえ埋めてあげれば、「あ、そゆこと？」となって自ら活動することが多い。
- その背景やそのインパクトを考えてメリハリあるセキュリティがおすすめです。
- そのためにも、ユーザーフレンドリーに、しっかりみなさんで考えるセキュリティを(部会やISACといった横断コミュニティで)。

目次

本セッションのゴール設計

言葉じりだけ先行するサイバーセキュリティ
実際のところどうなの？ってのを考えるきっかけに

＋

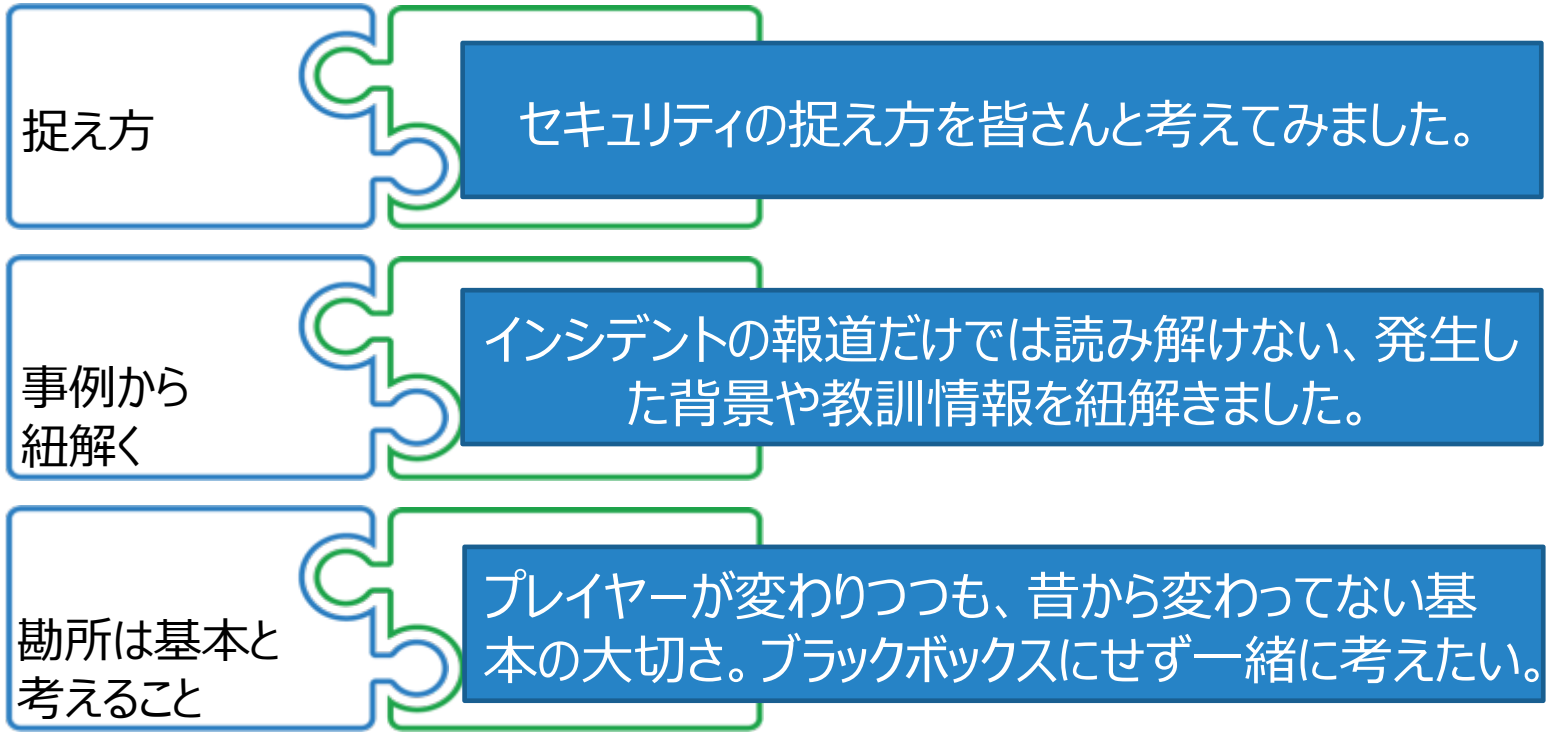
基本的な対策(全体設計、構成管理、ログ管理など)が大切

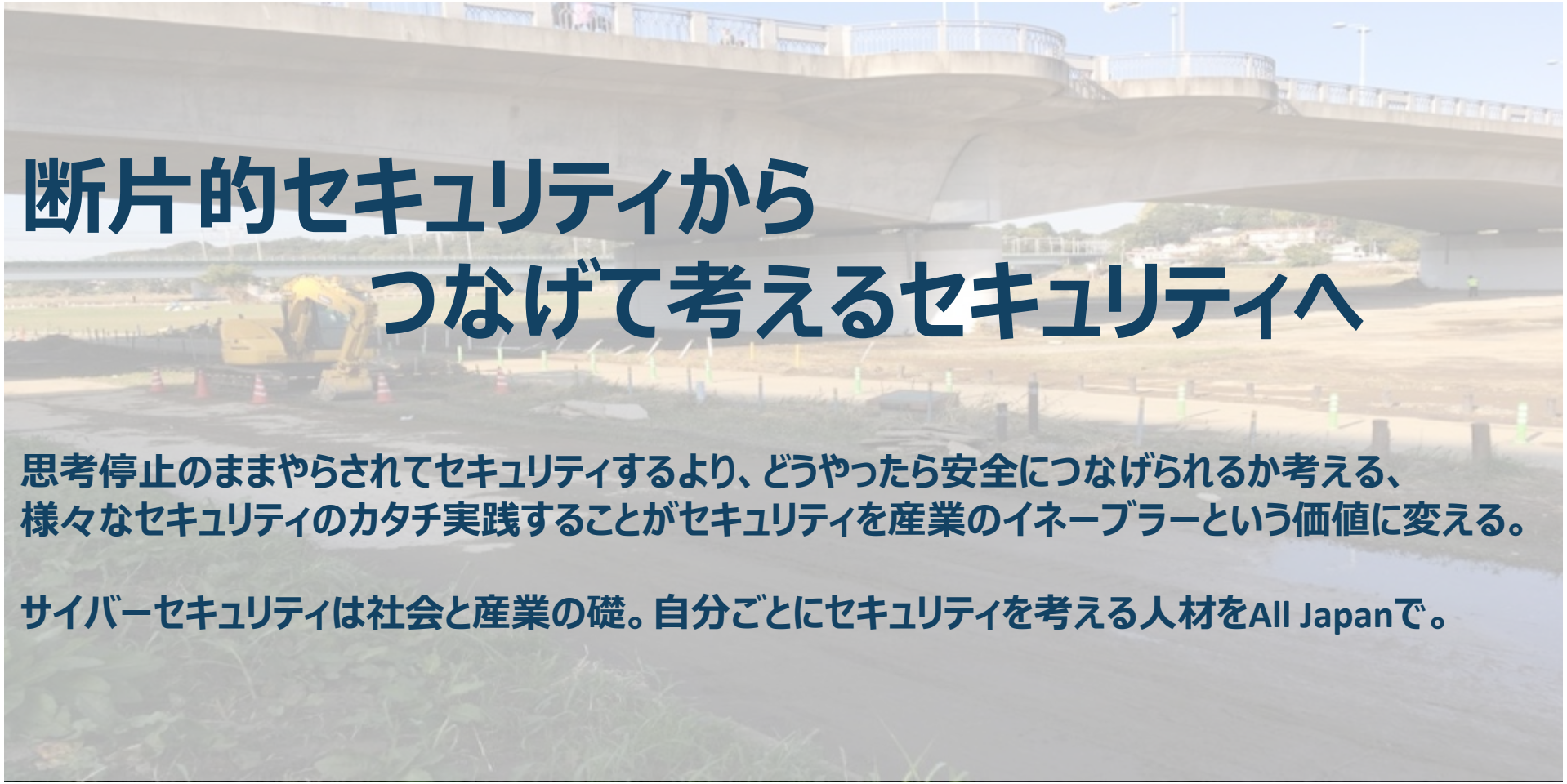
問いかけ⑦

本日、一番印象に残ったキーワードを挙げてください。

差し支えない範囲で、チャットにてコメントください。

さいごのまとめ





断片的セキュリティから
つなげて考えるセキュリティへ

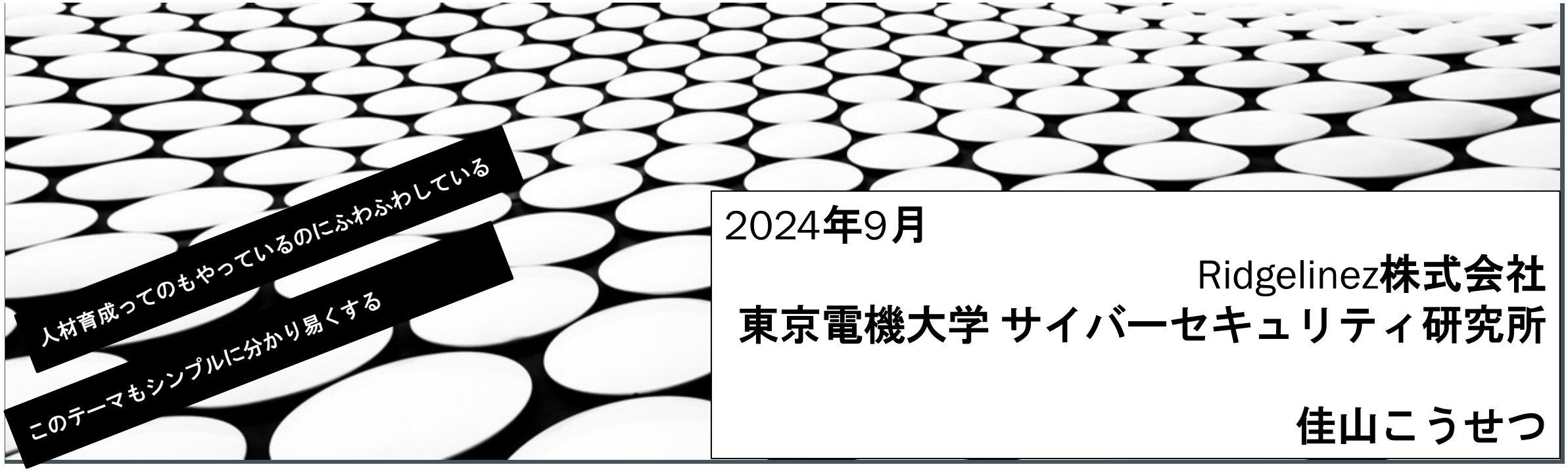
思考停止のままやらされてセキュリティするより、どうやったら安全につなげられるか考える、
様々なセキュリティのカタチ実践することがセキュリティを産業のイネーブラーという価値に変える。

サイバーセキュリティは社会と産業の礎。自分ごとにセキュリティを考える人材をAll Japanで。

FISAC金融部会 勉強会

延長戦：人材育成のお話

～どこか断片的な人材育成を考える～



2024年9月

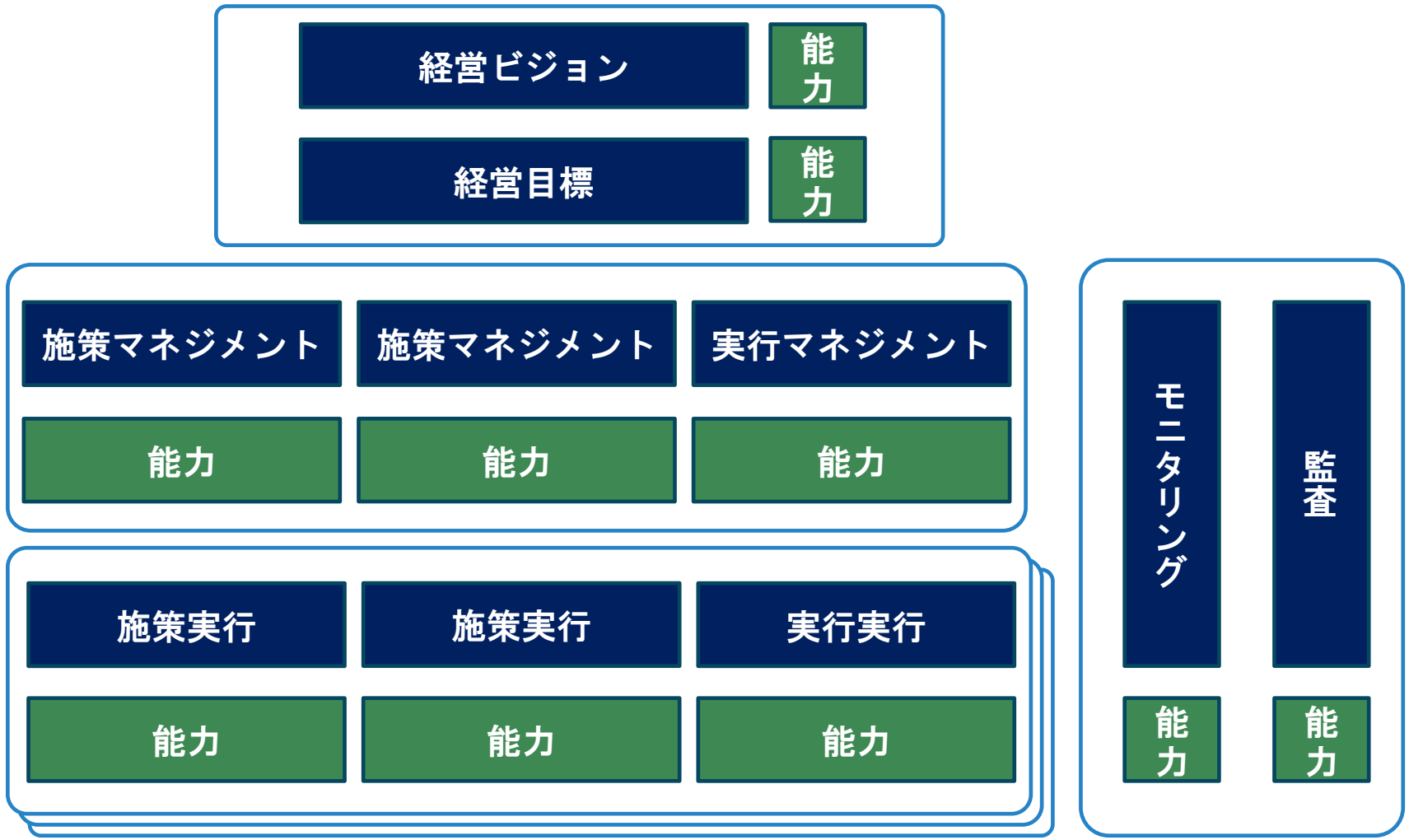
Ridgelinez株式会社
東京電機大学 サイバーセキュリティ研究所

佳山こうせつ

ひも解くヒント②：人材育成と企業ガバナンスは実はしっかりつながっている

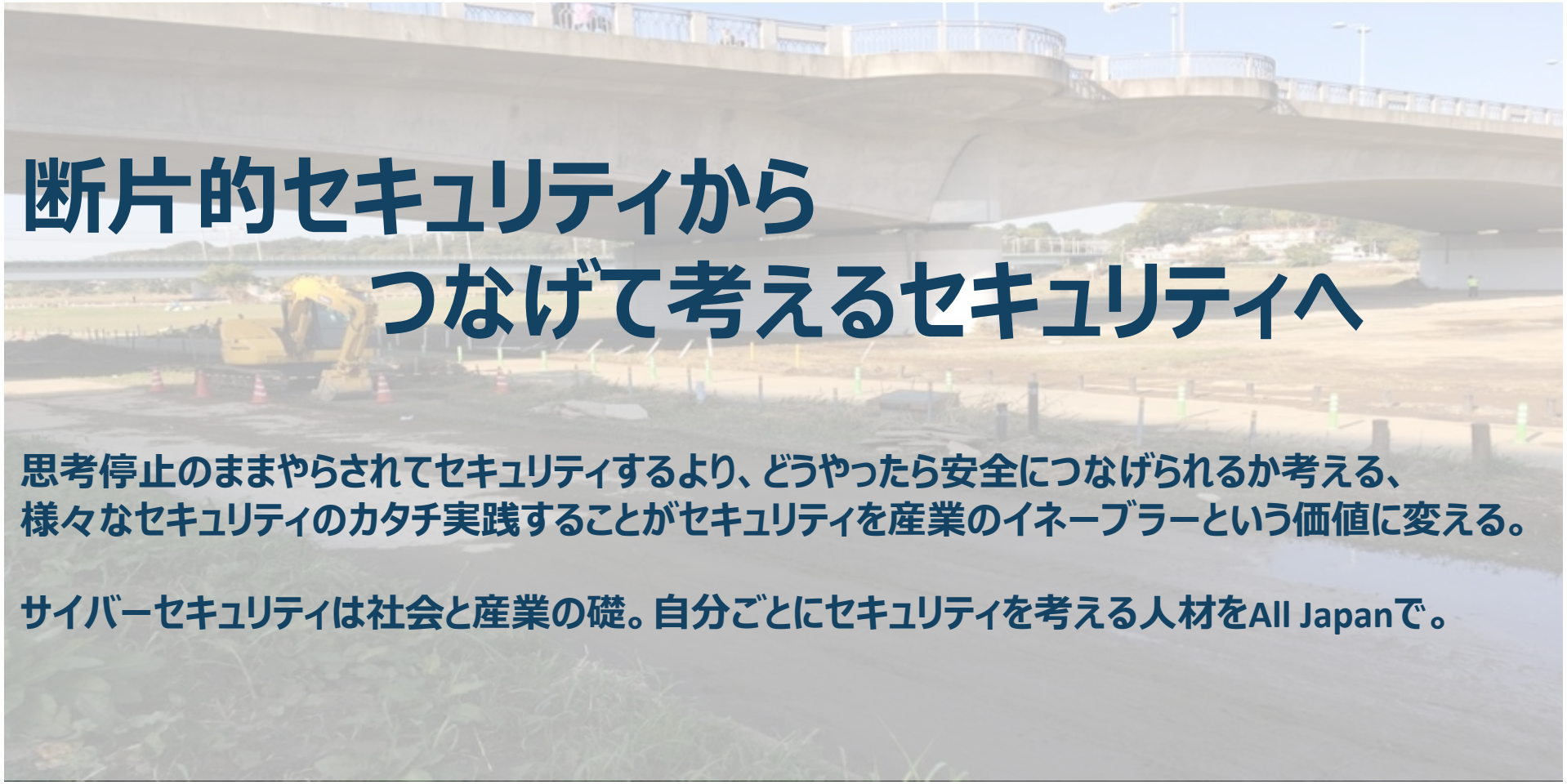
投影のみ

経営目標を達成するために必要な施策、その施策遂行のために必要な人材の能力といった形で因数分解することが効果的



ポイント

- 人材育成を目的としない、目的に合った人材育成
- セキュリティ施策も目的ではなく、経営に必要なガバナンス
- ガバナンストップから現場まで一貫した戦略に基づくしなやかな人材育成マネジメントが肝要
- ３線モデルごとに異なる人材像



断片的セキュリティから
つなげて考えるセキュリティへ

思考停止のままやらされてセキュリティするより、どうやったら安全につなげられるか考える、
様々なセキュリティのカタチ実践することがセキュリティを産業のイネーブラーという価値に変える。

サイバーセキュリティは社会と産業の礎。自分ごとにセキュリティを考える人材をAll Japanで。