

共通必要人材フレームワーク

Cyber Security Baseline Assessment for Cloud



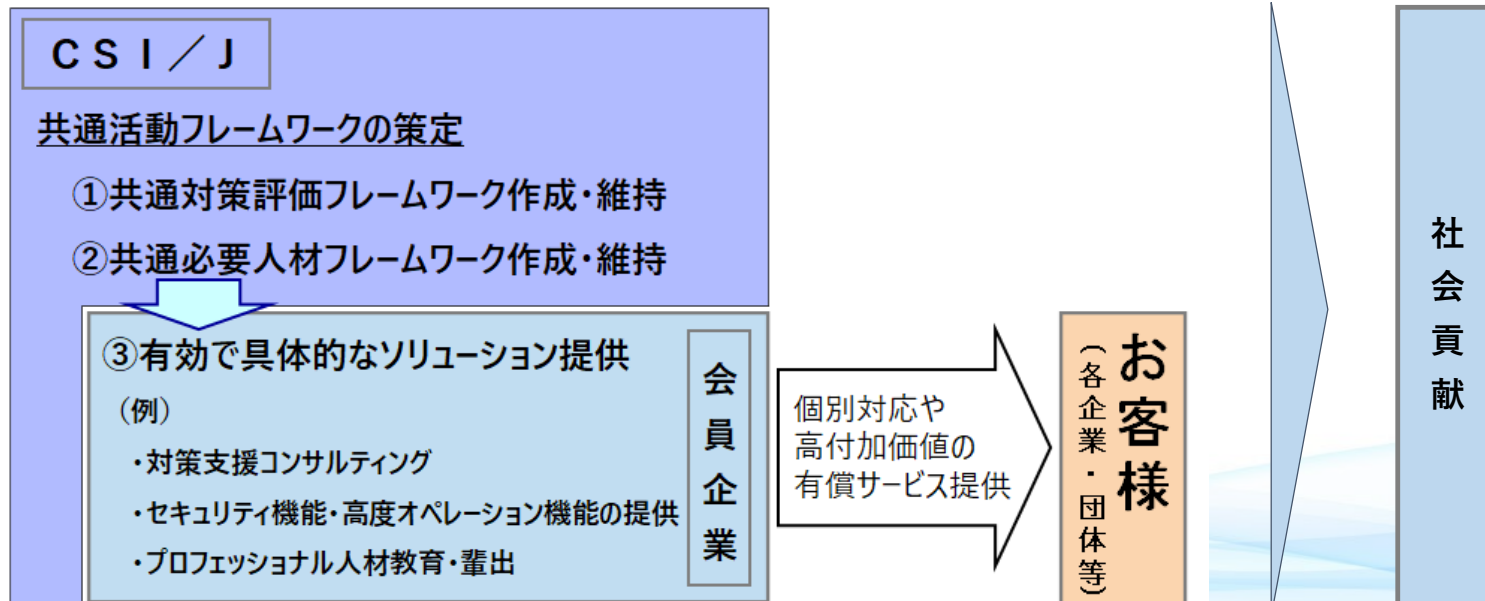
Cyber Security Initiative for Japan

企業における「セキュリティレベルの向上」を目指し、クラウド、ゼロトラスト、IoT、サプライチェーン等の新領域に対する「サイバーセキュリティ」対応を、セキュリティ業界横断で顧客企業への支援活動をおこなう

支援の切り口は以下の通り

- ①サイバーセキュリティ共通対策評価フレームワークの策定・維持
- ②共通必要人材フレームワークの策定・維持
- ③有効で具体的なソリューションの提供：会員企業（セキュリティベンダ）による

■活動概要



現代の課題に対応する有用なフレームを次々と発信

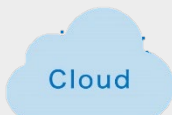
共通評価フレームワーク

【共通対策評価フレームワーク分科会】

第一弾

**クラウド環境を利用しようと検討中の企業
クラウドを利用しているが、安全性に不安のある企業**

- ・クラウドセキュリティのチェックを行う部署・担当の方
- ・クラウド利用を検討・推進している部署・担当の方
- ・クラウドサービスの企画、推進を行う方
- ・情報システム部門のリーダー、担当者 など



共通必要人材フレーム

【サイバーセキュリティプロフェッショナル人材フレームワーク分科会】

**セキュリティ人材の正確な価値が見える化
優良なセキュリティ人材の健全な育成**

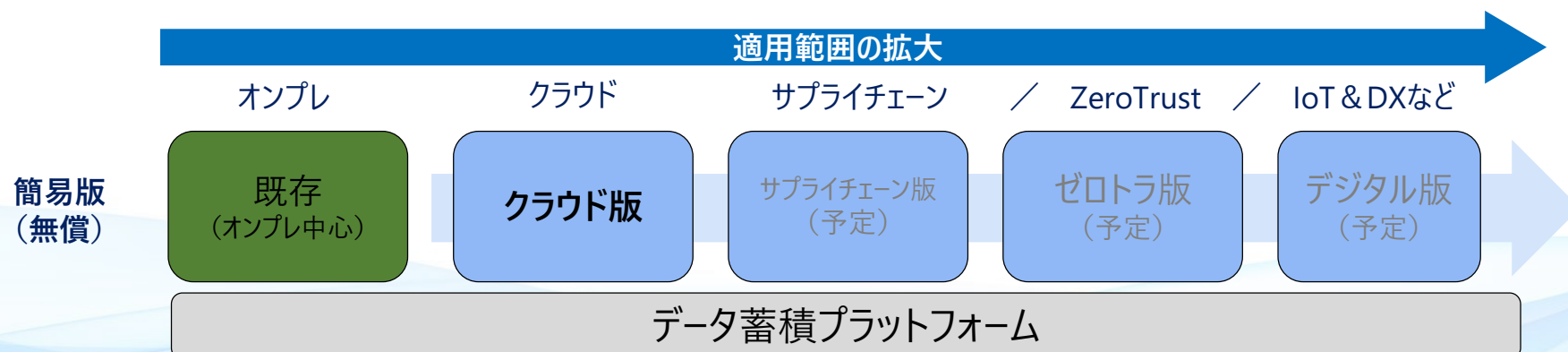
- ・セキュリティ人材の正確な価値を知りたい方
- ・優良な人材を所属する企業を選ぶ担当の方
- ・優良人材（特にエンジニア）になりたい、育成したい方
- ・人事部門長、セキュリティ人材育成担当者 など



今後も共通評価フレームワークは拡大していきます

適用範囲をクラウドからサプライチェーン・DXなどの環境変化・市場ニーズに合わせ拡大

お客様の現実的な実装に向けて、会員企業が用意する各ソリューションにて推進・支援してまいります。

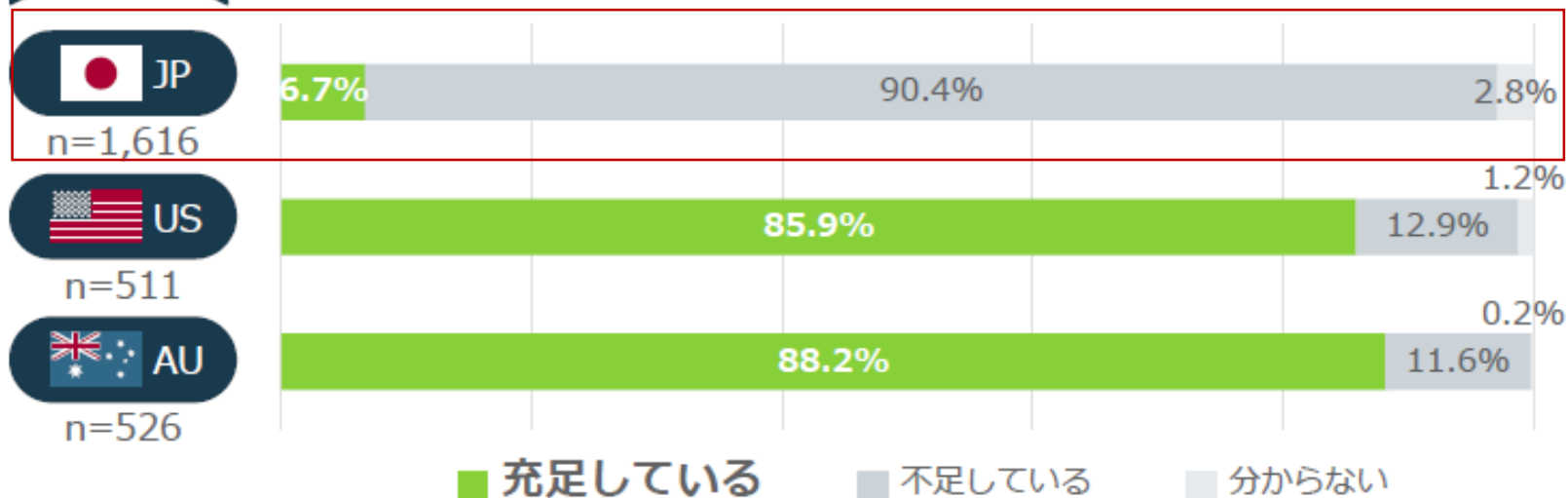


NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査2021」より
<https://www.nri-secure.co.jp/news/2022/0208>



セキュリティ対策に従事する人材の充足状況

90%以上の企業が不足していると回答



※充足している：「人材が過剰な状態」「充足している（最適な状態）」「どちらかといえば充足している」のいずれかを回答
※不足している：「どちらかといえば不足している」「不足している」のいずれかを回答

共通必要人材フレームワークとは：日本では長年セキュリティ人材不足がクローズアップされているが、2021年度の調査でも充足度は僅か6.7%と欧米諸国の80%台に比して極端に乖離している。いま企業が安全にITの利活用やDX推進を進める中で、必要となる「セキュリティ人材」を育て、増やしていくために、**専門性・耐用性が幅広くて分かりにくかった人材ロールを、実際の業務に焦点を当てることで分かりやすくし、**必要な能力を明確化する必要がある。さらにその人材を「どうすれば本当に育成できるのか？」学習体系まで明示した人材フレームが必要となる。これを「共通必要人材フレームワーク」として整備し、公開する。



- ・ プロとしてセキュリティに従事するエンジニアはどんなスキルが必要か？
- ・ 育成するプロセスはどう進めれば良いか？

【ロールの選定基準】

- 従来から需要が高く人材の育成が急がれるロール
- セキュリティ体制の構築にあたって重要な役割を果たすロール
- 環境変化に迅速に追従できる先進的なセキュリティを実現するロール

などなど…

このようなお悩みの
指標となるフレームワークを！

共通必要人材フレームワーク

- ・ セキュリティ技術者としてのロールと必要なスキルを定義
- ・ 学習するステップを体系化してシンプルに明示
- ・ 選定するロールは「激しい環境変化に対応するためのロール」が中心

必要な人材と 育て方



日本の人材不足を解消するために：CREDO

このフレームワークによって、セキュリティ人材の育成に貢献する。
さらに将来的には、それぞれ定義したロールが「サイバーセキュリティプロフェッショナル」としてのブランドを確立することで、セキュリティ人材全体の価値向上を実現し、異業種からもセキュリティエンジニアを目指す人が増え、日本の根強い人材不足を改善する。

激しい環境変化に対応するための人材を⇒現場の悩みにフォーカスしたロールを厳選

ロールの選定基準：

- ・従来から需要が高く人材の育成が急がれるロール
- ・組織にセキュリティ体制の構築にあたって重要な役割を果たすロール（需要の大小に関わらず）
- ・次世代に必要と目される先進的なセキュリティを実現するためのロール

①各ロールごとに2つのレベル（エントリー/マスター）を定義



インシデントハンドラ



Web/NW脆弱性診断士



情報システムペンテスター



IoT脆弱性診断士



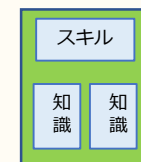
IoTシステムペンテスター



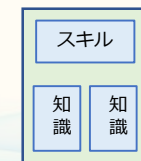
匠の会



マスター



エントリー

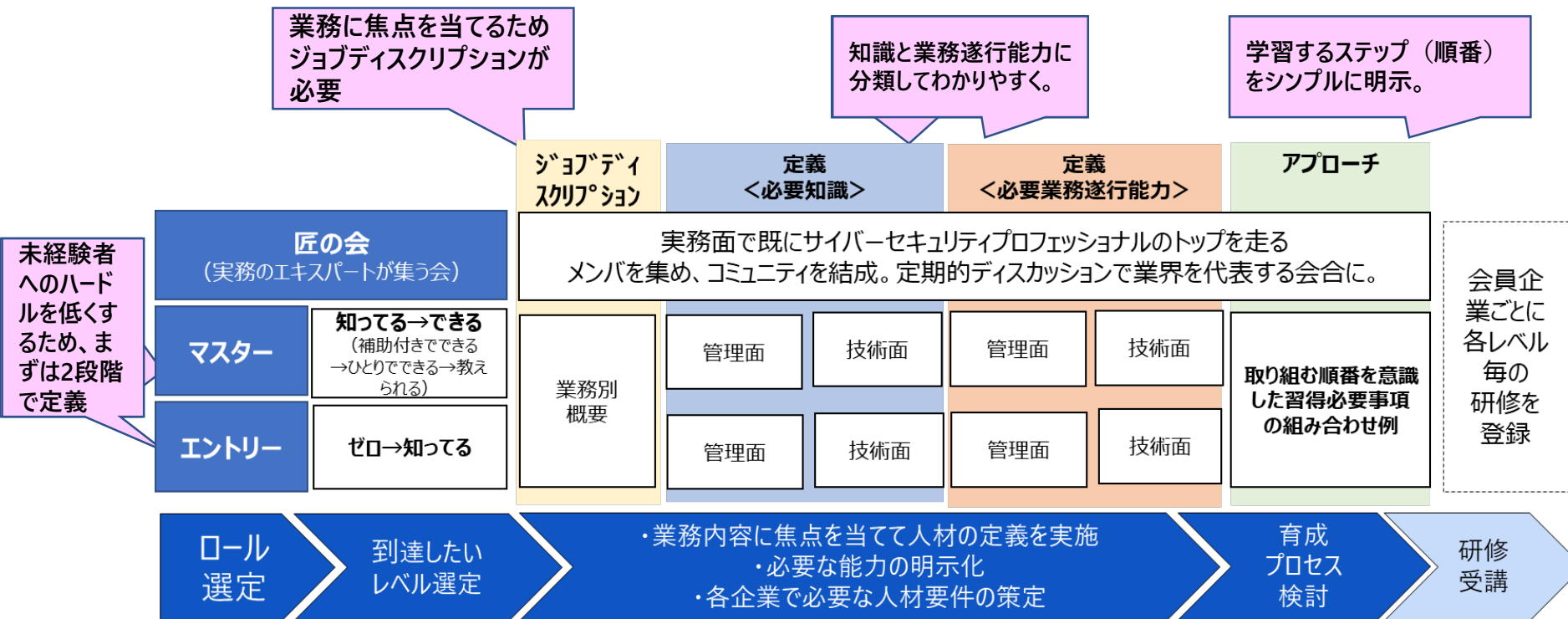


③プロが集まる
コミュニティを
立ち上げ

②各レベル別に
必要な知識やスキル
育成プロセスを定義

全体像

分からない → 知っている → できる までを体系化



業務の視点でフォーカスした人材ロール
各ロールを2段階のレベルに分け、明確に定義
育成プロセスまで具体化して明記

⇒ 変化に追従でき、活用し易い
⇒ シンプルで分りやすい
⇒ より効率よく育成できる

共通必要人材フレームワーク 各ロールの定義シート



シンプルでポイントを押さえた
ジョブディスクリプションと定義

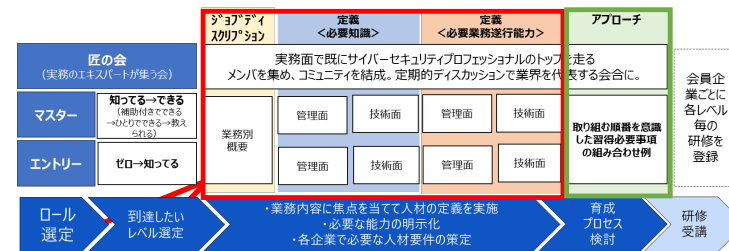
●ロールごとに定義

- ・ジョブディスクリプション
- ・レベル別定義（知識・業務遂行能力）
- ・アプローチ（カリキュラム）

ジョブディスクリプション・定義（例：Web/NW脆弱性診断士の場合）

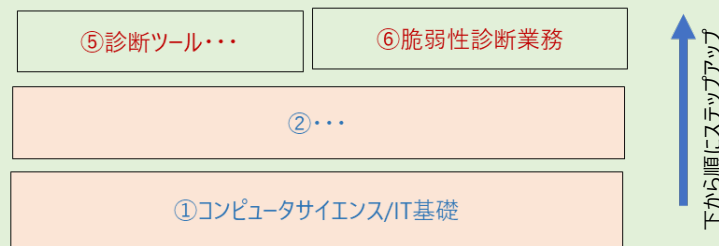
定義			
ジョブディスクリプション		ITシステムの脆弱性診断を実施 ・Webアプリケーションやプラットフォームの脆弱性やセキュリティ機能の調査 ・脆弱性診断の報告書の作成と説明、対策の提言	
エントリー	業務遂行能力	管理	上位のサポートにより以下を部分的に実施できる ⑥脆弱性診断業務（情報収集・報告書作成・リスク評価） -脆弱性に・・・
		技術	上位のサポートにより以下を部分的に実施できる ⑤診断ツールの使用 -診断環境に応じて、・・・
	知識	管理	④脆弱性診断業務（診断計画・リスク評価）に関する知識 -診断の業務フローを・・・ -診断対象の画面、リクエスト、アクション、パラメータを・・・
		技術	①コンピュータサイエンス/IT基礎 -標準的なプロトコルと技術の用途や特徴、・・・ -ネットワークセキュリティ技術の・・・

人材フレームワークの全体像



アプローチ

（習得の順番を表しています。下から順番に習得するのが推奨です。）



●エントリーはWebサイトで公開（リリース済み）

URL：<https://www.csi-japan.org/csprohuman>

マスターは会員企業向けに公開

●今後、さらに各ロール毎の 次のキャリア例 を提示し、その先の成長を明示

未経験者でもわかるように
習得する順番・プロセスを重視
シンプルなカリキュラムを
各ロールごとに提示

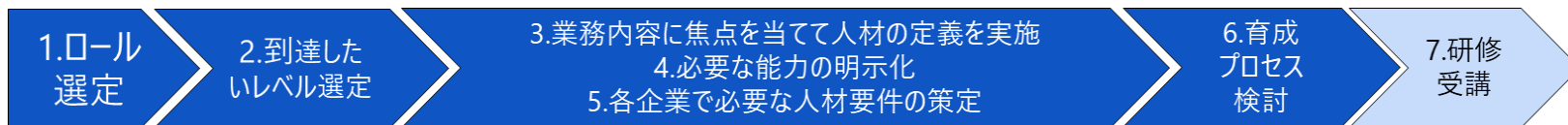
①

- インシデントハンドラ
- Web/NW脆弱性診断士
- 情報システムペンテスター
- IoT脆弱性診断士
- IoTシステムペンテスター

[illegible]

© 2022 CSIJ.

フレームに沿った事例 1 (A社) 目的：CSIRTチームメンバの育成・増員



1. ロールとして「インシデントハンドラ」を選定

2. As Is: 現状1名 + 兼務1名

To Be: 管理者1名 + 実務対応者3名の体制を今年度中に構築したい。エントリー2名/マスター1名。

⇒ 候補人材：元IT部員（3名）うち1名セキスペ保有

3.～5. セキスペ保有者をマスター候補（マネージャ候補）に、他2名をエントリー候補。

⇒ さらに業務経験や知識を精査したところ、エントリーの③～⑪を習得させる必要あり。

うち、特にエントリー候補は知識④と⑦～⑩の遂行能力が必要。

6. セキュリティベンダへ相談

⇒ 人材育成コンサルティングサービスを利用し中期育成計画を立て、B社のトレーニング受講

7. 知識④と⑦～⑩の遂行能力を身に着けるため以下を受講する予定。

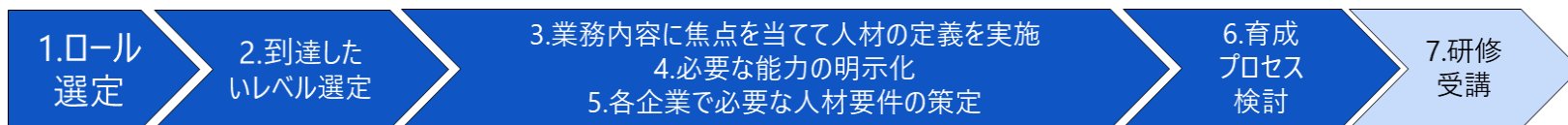
⇒ ○月のSecureEggs IT + セキュリティ基礎 2名受講

⇒ ○月のSANS FOR508 1名受講

フレームワークと会員企業の有償サービスを活用し
短期間に効率よく育成を進め、体制構築を実現！

インシデントハンドラ		研修メニュー				
スキル	項目	SecureEggs IT+セキュリティ基礎	SecureEggs インシデント対応	SecureEggs フォレンジック	SANS FOR508	SANS FOR508
		○	○	○	○	○
管理 能力	インシデントハンドリングと対応の仕組み、業務委託時のNDA等に関する理解と実施				○	○
	第一線のインシデント対応の実務				○	○
	インシデント対応において行われる各種エスケーシングの遂行		○		○	○
	①情報セキュリティに関する総論とトピックス				○	○
実務 能力	②情報セキュリティに関する総論とトピックス				○	○
	③情報セキュリティに関する総論とトピックス				○	○
	④情報セキュリティに関する総論とトピックス				○	○
	⑤情報セキュリティに関する総論とトピックス				○	○
知識	⑥情報セキュリティに関する総論とトピックス				○	○
	⑦情報セキュリティに関する総論とトピックス				○	○
	⑧情報セキュリティに関する総論とトピックス				○	○
	⑨情報セキュリティに関する総論とトピックス				○	○
その他	⑩情報セキュリティに関する総論とトピックス				○	○
	⑪情報セキュリティに関する総論とトピックス				○	○
	⑫情報セキュリティに関する総論とトピックス				○	○
	⑬情報セキュリティに関する総論とトピックス				○	○

フレームに沿った事例 2 (B社) 目的：セキュリティ診断ができる協力会社の増員



1. ロールとして「Web/NW脆弱性診断」を選定

2. As IS: 診断メンバは現状〇名。

To Be: 年度末の多数の案件に対応するため、エントリーを2名育成を目標とする。

⇒ 診断を行っている社員の補助ができるようになる

3.～5. 候補人材：エントリーの①～③はすでに身につけているが、③～⑥は未習得。

⇒ 3か月後までに⑥までの習得は必須

6.7. 8月のSecuriST Webアプリ脆弱性診断士を受講させる。

⇒9月～10月 実際の診断案件に補助として参画し実践経験を積む

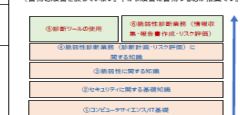
⇒ 10月末までにWebアプリ診断10件を経験

セキュリティベンダにも適用可能!

フレームワークと会員企業の有償サービスを活用し
短期間に効率よく育成を進め、体制構築を実現!

● Web / NW開発性診断士

アプローチ
(買手の順番を決めています。下から順番に買渡るのが特徴です。)



Secu072E Webアプリケーション 脆弱性診断	Secu072E 4.0.0 脆弱性診断	Secu07 2.4.0 Webアプリケーション 脆弱性診断
○	○	
○	○	
○	○	
○	○	○
○	○	○
○	○	○

ちゃんとインシデント対応できるようになりたい



・インシデントハンドラ

IoTは複雑だけどセキュリティテストしなきゃ



・IoT脆弱性診断士

人材フレームワークで



勉強の仕方が分かる！

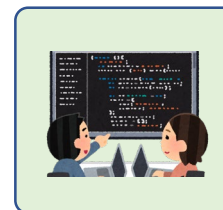


ジョブロールごとに
必要な学習方法が分かる

どんなトレーニングが
最適か分かる



講習による効率的な学習



ハンズオンによる経験



ワークショップで体得



会員企業による有償育成サポート

■Vision 実現したい未来

- ・セキュリティ人材がデジタル社会の実現に向け**必要不可欠な存在**となる

■Mission 果たすべき使命

- ・セキュリティ人材の価値向上とセキュリティ人材不足の解消を目指す

■Value 約束する価値・強み

- | | |
|------------|--------------------------------------|
| ・社会ニーズの重視 | 実社会に不足する人材、必要とされる人材の育成を重視する |
| ・キャリアパスの提示 | 未経験からのエントリーからその先の成長までのつながり・プロセスを提示する |
| ・シンプルな内容 | 未経験者や人材を採用する企業でも使えるシンプルで活用しやすい内容にする |
| ・魅力の発信 | 多くの人が興味を持ち、魅力を感じてもらうために情報を発信する |

Thank you. Any Questions ?

- セキュリティ技術者のプロフェッショナルなロールを定義
- 学習するステップを体系化してシンプルに明示



Cyber Security Initiative for Japan