ホワイトハッカーの世界へようこそ

女性活躍推進×サイバーセキュリティ――新しい可能性

女性活躍支援コンソーシアム 特別講習

株式会社 Trive 常務執行役員社長補佐兼CTO
株式会社 Trive Secure Lab 執行役員副社長

桑原 義幸, CISSP

所要時間：約45分

Career Journey

Trive Secure Lab（TSL）とは？

広島から、世界水準のサイバー防衛を

ミッション：最先端の技術と揺るぎないコミットメントで、日本のサイバーセキュリティを守る

広島、ここを防御の聖地とす　／　多様な個の力を磨く（エイジレス・ジェンダー）　／　世界と連携した最前線の技術

会社概要

左：代表取締役CEO　増田 剛洋
右：副社長 桑原 義幸

会社名	株式会社 Trive Secure Lab
設立	2025年9月1日
所在地	広島市南区京橋町1-7（fabbit 広島駅前）
代表者	代表取締役 CEO　増田 剛洋
資本金	2,000万円（株式会社Trive 100%出資）

事業内容

1. サイバーセキュリティ コンサルティング
2. セキュリティ診断
   （脆弱性診断・ペネトレーションテスト等）
3. セキュリティシステムの企画・開発・設計
   ・製造・販売・保守及び管理
4. サイバーセキュリティに関する
   研究開発及び教育

なぜ、私たちは Wales なのか？　－　150年の必然

⚓ 1871年

東郷 Wales留学

明治の海軍士官・東郷平八郎がWalesで7年間学ぶ。日本海海戦「T字戦法」の礎に。

⚔ 1877年

戦艦「比叡」建造

Walesの職人の鉄と技術が太平洋を渡り、日本の盾となった。技術は国境を越える。

🌿 2020年頃

イチョウ、呉へ帰還

東郷が帰国時に植樹したいちょうの分け木が、英国海軍将校と共に呉に植樹された。

2026年―この150年の絆が、Cyber Wales × TSL のサイバー同盟として結実した

150年の絆が、現代のサイバー防衛へ

Wales × JP 広島・呉――歴史は必然を語る

1871年

1 東郷平八郎、英国ウェールズへ留学

明治の若き海軍士官が7年間Walesで学ぶ。造船・航海術・海軍戦略を習得。「日本のネルソン」はウェールズで生まれた。

1912年

2 戦艦「比叡」、Walesで建造→太平洋へ

英国ヴィッカース造船所で建造。ウェールズの職人の技術と鉄が日本の盾となった。日英の「共に守る」精神の象徴。

2020年頃

3 イチョウの苗木、呉に帰還

1878年に贈られた苗木の分け木が英国海軍将校×呉市長立会いのもとで植樹。150年の絆が現代に可視化された。

2026年～

4 Cyber Wales × TSL――サイバー防衛同盟へ

英国政府公認のCyber WalesとTSLが正式提携。SudoRangeを活用したホワイトハッカー育成を広島から全国へ。造船→サイバーへ、絆は続く。

Cyber Wales：英国政府公認・1,000社以上集積するサイバー拠点。NATO・EU防衛にも貢献。アジア唯一の正式パートナーが広島のTSL。

そもそも「サイバーセキュリティ」って何？

まず基礎から整理しましょう――職場への紹介にも使えるたとえです

インターネットやコンピュータを使う「デジタルの世界」を
悪意のある攻撃や事故から守る、すべての取り組みのこと

わかりやすく言うと――

現実の世界		デジタルの世界
🏠 家に鍵をかける	→	🔐 パスワードを設定する
🚗 車にセキュリティをつける	→	🛡 ウイルス対策ソフトを入れる
🏢 銀行が金庫を管理する	→	💾 企業が顧客データを守る
👮 警察が犯罪を取り締まる	→	🧑‍💻 ホワイトハッカーが攻撃を防ぐ

現実の世界でやることが、デジタルでも必要になっている――それだけです！

今、世界と日本で何が起きているか

数字で見るサイバーセキュリティの「危機」と「チャンス」

6兆

ドル/年

サイバー犯罪による
世界の被害額（2023年）
日本のGDPの約1.5倍！

1分に4回

世界のどこかで
サイバー攻撃が
発生している頻度

約40万

人不足

日本が今すぐ必要とする
セキュリティ人材数
（経産省調査）

「40万人不足」は、裏を返せば――

40万の『空席』――貴社・貴自治体の女性人材が担える可能性があります！

「対岸の火事」ではない

2022〜2024年、実際に起きたサイバー事故

2024年6月

KADOKAWAグループ

ランサムウェア攻撃

ニコニコ動画など全面停止。25万人以上の個人情報流出。復旧まで2ヶ月以上。

大手でも一夜にしてサービス全停止

2024年10月

カシオ計算機

ランサムウェア攻撃・情報漏洩

従業員・取引先・顧客情報が漏洩。発売予定商品の延期、修理システム停止。

製造業でも個人情報・内部文書が標的

2023年7月

名古屋港（NUTS）

ランサムウェア攻撃

コンテナターミナルが約3日間停止。搬出入全面中止で物流に甚大な影響。

港湾インフラへの攻撃で国内物流が麻痺

2024年12月

日本航空（JAL）

DDoS攻撃・システム障害

年末年始ピーク時にシステム障害。フライト遅延・欠航が多発。

航空インフラも攻撃対象。命に関わるリスク

2024年5月

岡山県精神科医療センター

ランサムウェア攻撃

電子カルテが停止。約4万人分の患者情報が流出の可能性。医療現場が麻痺。

病院への攻撃は患者の命を直接脅かす

2022年〜継続

大手自動車メーカー（サプライチェーン）

サプライチェーン攻撃

取引先が攻撃され国内全工場が一時停止。自社対策だけでは防げない脅威。

自社が安全でも取引先経由で被害を受ける

⚠ IPA「情報セキュリティ10大脅威 2025」ランサムウェアは10年連続1位。2025年上半期だけで国内247件のインシデントが公表されています。

自治体も例外ではない

～住民情報・行政サービスを狙った攻撃が急増中～

2024年5～7月

全国複数の自治体

委託先（印刷会社）経由のランサムウェア被害

印刷・発送業務を委託していたイセトー社がランサムウェアに感染。納税通知書・ワクチン接種関連データなど住民の個人情報が流出した可能性。自治体自身は何もしていないのに被害を受けた。

自治体の「委託先管理」が問われた事例

2024年11月

熊本県

農業関連サイトへのDDoS攻撃・情報流出

県が管理する農業関連サイトが大量アクセス攻撃でダウン。その後、住民の氏名・住所など数千件の個人情報が流出した可能性が判明。委託先のセキュリティ不備が原因と指摘された。

住民の氏名・住所が流出――委託先管理の不備

2024年秋～継続

国内複数の自治体・交通機関

ロシア系グループによるDDoS攻撃

ロシア系とみられる攻撃グループが国内自治体・交通機関のウェブサイトへ次々とDDoS攻撃を実施。サイトが閲覧不能となり業務が数時間停止するケースが相次いだ。政治的主張を兼ねた攻撃のため予告なく標的が変わる。

地政学リスクが自治体サイトを直撃する時代

住民情報という最高機密

氏名・住所・マイナンバー・税情報・医療情報――自治体が保有するデータは住民生活のすべてを含む。

委託先経由の「もらい事故」

印刷・システム・清掃……多くの業務を民間委託する自治体は、委託先のセキュリティ事故の影響を直接受ける。

行政サービス停止＝住民生活への直撃

給付金・災害対応・証明書発行――サイバー攻撃でシステムが止まると、住民の命に関わる行政サービスが麻痺する。

政府機関等へのセキュリティインシデント報告件数：2022年度 266件 → 2023年度 233件 → 2024年度 447件（前年度比 約1.9倍）　出典：内閣サイバーセキュリティセンター（NISC）2025年6月

事故が起きると、企業や自治体はどうなる？

お金だけじゃない――見えない損害の方が大きい

直接的な金銭的損害

- 身代金の支払い：数百万～数億円
- システム復旧費用：数千万～数億円
- 被害者への賠償金・法的費用

事業の停止・機会損失

- サービス停止による売上ゼロ（KADOKAWAは2ヶ月超）
- 復旧期間中の人件費・運営コスト
- 発売予定商品の延期による機会損失

信頼・ブランドの失墜

- 顧客離れ・株価下落（上場企業は即日影響）
- メディア報道による「炎上」リスク
- 採用活動への影響（優秀な人材が来なくなる）

法的・行政的リスク

- 改正個人情報保護法による行政罰・課徴金
- 取引先・顧客からの損害賠償請求
- 経営者・役員の個人責任が問われるケースも

中小企業の場合、サイバー攻撃1件で「廃業」に追い込まれるケースも。もはや他人事ではありません。

では、どうサイバー攻撃に立ち向かうか？

「備え」と「対応力」と「先手」の3層が必要

👑 攻めない・侵入させない（予防）

Layer 1

強固なパスワード管理・システム設計・社員教育・定期的な脆弱性チェック

家に強い鍵をつけて、窓に格子をつけるイメージ

🛡 早く気づいて・素早く対応する（検知・対応）

Layer 2

24時間監視（SOC）・攻撃を検知したらすぐ遮断・インシデント対応チーム（CSIRT）

火災報知器＋消防士のチームをいつも備えるイメージ

⚔ 攻撃者の手口を知る・先手を打つ（エシカルハッカー）

Layer 3

侵入テスト・脆弱性診断・バグバウンティ――わざと攻撃して弱点を見つける

泥棒役を雇って「どこから入れるか」を事前に調べるイメージ

▶ **Layer 3を担うのが「エシカル（ホワイト）ハッカー」です！次のスライドから詳しく見てみましょう。**

エシカルハッカー（ホワイトハッカー）の仕事

「悪い人の手口」を使って「良いこと」をする専門家

企業や自治体から「許可」をもらい、正式に依頼を受けてシステムに侵入・攻撃を試みる
―「正義のハッカー」―

侵入テスト（ペネトレーションテスト）

企業のシステムに「わざと」侵入してみる。どこから入れるか発見し修正を提案する。「泥棒さん役」の専門家。

脆弱性診断

アプリやウェブサービスの「穴」をチェック。患者の健康診断のように、弱いところを全部リストアップして報告する。

セキュリティ監視（SOC）

24時間システムを見張る「監視カメラ担当」。不審な動きを検知したら即対応。AIと人の目で守る。

インシデント対応（CSIRT）

攻撃を受けたときの「消防士」役。被害を最小限に抑え原因を調べて再発を防ぐ。スピードが命。

なぜ、この仕事は女性に向いているのか？

貴社・貴団体の女性人材に当てはまる強みはありませんか？

細やかな注意力・観察眼

ログの中の「小さな異常」を見つける力。「なんか変」に気づく感性が、セキュリティ診断で絶大な武器に。

→ SOCアナリストに求められる最重要スキル

コミュニケーション・伝える力

技術的な発見を「経営者にわかる言葉」で伝える。報告書作成・顧客対応・チームワークで輝く。

→ 技術だけでなく「橋渡し」ができる人材が希少

多様な視点・発想力

攻撃者はあらゆる手口を試す。男性だけのチームでは気づかない「盲点」を女性視点で発見できることも。

→ ダイバーシティがセキュリティそのものを強化する

文系・未経験・育児中でもOK

必要なのは「論理的に考える力」と「好奇心」だけ。元銀行員・元デザイナーで活躍している先輩が実在する。

→ 「理系でないと無理」は完全に古い思い込み

ある女性ホワイトハッカーの1日 ①

A子さん（32歳）

SOCアナリスト

- 📍 元・銀行員（文系出身）
- 🎓 育児休暇中に独学でIT学習
- 📜 CompTIA Security+ 取得
- 💼 現在3年目・チームリーダー
- ⏰ 時短勤務・2児の母

09:00 — **SOCダッシュボード確認**
夜間のアラートをチェック。異常なログイン試行が300件。「これ、怪しい……」

09:30 — **不審アクセスの分析・対処**
海外IPからのブルートフォース攻撃と特定。すぐにブロックリストを更新して撃退！

11:00 — **最新の攻撃情報をチェック**
国内外の脅威情報を確認。同じ攻撃が他社でも発生中と把握し注意喚起メールを作成。

13:30 — **経営層向けレポート作成**
「何が起き、どう対処したか」を難しい言葉なしでまとめる。コミュ力が光る場面！

15:00 — **後輩のメンタリング**
後輩の女性スタッフにSOC業務を指導。「私もはじめは全然わからなかったよ」と笑顔で。

17:00 — **定時退勤・保育園お迎え**
「守りたいのは会社のデータだけじゃなくて、家族の時間も」——時短でしっかり定時！

ある女性ホワイトハッカーの1日 ②

B子さん（28歳）

ペネトレーションテスター

- 📍 元・Webデザイナー（美大卒）
- 🎓 CTF大会参加がきっかけで転職
- 📜 CEH（倫理的ハッカー）取得
- 🌐 フリーランスでも活動中
- 💰 年収：前職の2.3倍に上昇

09:00 クライアントとキックオフMTG
「今日から御社のシステムに侵入を試みます」――これが正式な仕事の始まり！

10:00 偵察フェーズ（公開情報を調べる）
ウェブサイト・SNSで攻撃の糸口を探す。デザイナー経験がUI分析に活きる！

11:30 脆弱性スキャン実施
ツールでシステムの弱点を自動検出。「ここ、パスワードが簡単すぎる……」

13:30 侵入テスト本番
見つけた弱点を実際に突いてシステム内部へ。どこまで侵入できるか確認する。

15:30 わかりやすい報告書を作成
発見した問題を「専門家じゃない人でも読める」言葉と図でまとめる。美大出身が活きる！

17:30 CTFで腕を磨く
仕事後もハッキング競技に参加。「強い攻撃者の思考を学ぶには、戦うのが一番！」

CYBER SAMURAI PROGRAM™

セキュリティの基礎から段階的にステップアップできる「エシカルハッカー」育成プログラム

攻撃者の視点を学び、未知の脅威に対し自律的に判断・防御できる「即戦力の技術者」を育成する。

年齢や性別を問わず、情報資産を守る真の「サイバー侍」を輩出する、教育と実戦が融合したプログラム。

基本スキル習得プログラム
セキュリティへの関心

CYBER SAMURAI PROGRAM™
セキュリティスキル向上

LAB訓練 Capture the Flag（SudoCyber）
現場レベルの経験蓄積

プロフェッショナル
安心・安全の内製化

コホート型集合教育

5〜10名のクラス制を採用。互いに切磋琢磨する環境を作り、リード講師・メンターが手厚くサポート。

倫理教育の徹底

技術力だけでなく、ハッカーとしての「行動規範」と「誇り」も醸成する「White Hat」カリキュラム。

CYBER SAMURAIとは何か – Cyber SAMURAI Framework -

かつての武士は、己を鍛え、組織を守り、社会を守った。
Cyber SAMURAIは、その精神をサイバーの時代に再解釈した存在である。

S	**Strategy**	（戦略）	サイバーリスクを経営課題として捉え、戦略を策定する
A	**Architecture**	（設計）	ゼロトラスト等に基づき安全なシステム構造を設計する
M	**Monitoring**	（監視）	SOC等により脅威を常時検知・可視化する
U	**Unified Response**	（統合対応）	CSIRTにより統合的にインシデント対応を行う
R	**Resilience**	（回復力）	被害発生後の迅速な復旧・事業継続を実現する
A	**Awareness**	（意識醸成）	社員教育・演習を通じてセキュリティ意識を高める
I	**Intelligence**	（脅威情報）	脅威インテリジェンスを活用し先手を打つ

CYBER SAMURAI PROGRAM™ — Level 1〜3

ゼロから「侵入テスト」まで、段階的に着実にステップアップ

Level 1 入門

Basic ／ 16〜20時間

- サイバーセキュリティの基本的な知識
- サイバーセキュリティにおける組織のコンプライアンス
- サイバーリスクおよび脆弱性の管理
- コンピュータ操作の基礎（Windows編）
- コマンドラインの基礎（Linux編）

「怖いもの知らずで触れる」自信をつける

Level 2 実践

Essential ／ 50〜54時間

- ペネトレーションテストの基礎
- Kali Linux入門とハッキングラボを使った基本トレーニング
- ペネトレーションサービスの実践
- サイバーセキュリティにおける高度な処置
- Hackerに必要なマインド・フォレンジック入門

「本物のツール」で攻撃と防御を体感する

Level 3 上級

Expert ／ 30〜34時間

- ハッキングラボでのトレーニングに向けたメンターシップ
- "Ninjya" の基本操作
- "Metasploit Deeper" の基本操作（ピボッティング・C2）
- Windowsエスカレーションのテクニック
- 高度な侵入シナリオへの対応

「実戦レベル」の思考と技術を習得する

CYBER SAMURAI PROGRAM™ — Level 4

Level 3修了後、「攻撃系」か「防御系」か——自分の強みで専門家へ

Level 3まで修了したあなたは、2つのルートから専門分野を選べます

⚔ 攻撃系（Hacker）

CEH相当の技術力を習得

- Exploit開発技術
- EDR回避・Hooking技術
- 高度な攻撃シミュレーション
- 最新ツール（Metasploit・Ninjya）実践
- CTF（Capture the Flag）競技への参加

目標資格：CEH（認定エシカルハッカー）

🛡 防御系（Professional）

CISSP相当の知識を習得

- SOC業務（ログ解析・脅威ハンティング）
- セキュリティガバナンス・リスク管理
- 組織マネジメント能力
- インシデントレスポンス体制の構築
- セキュリティポリシー・法規制対応

目標資格：CISSP（認定情報システムセキュリティプロフェッショナル）

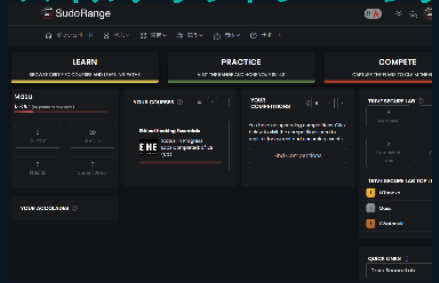
SudoRange™ — 英国発・クラウド型学習プラットフォーム

ゲーム感覚で学べる、本物のサイバー演習環境

SudoCyber（英国ウェールズ・ブレコン発）

元英国軍関係者が設立。Co-Founder & CEO：John Davies MBE ／ CTO：Jason Davies。英国警察・軍・大学・民間企業への豊富な実績。国家レベルの脅威対抗経験と最新技術を融合。

スキルアップトレーニング



実戦形式でのスキル習得ができるトレーニング。Webアプリでいつでもどこでも受講可能。

LEARN → PRACTICE → COMPETE

実践訓練 LAB

ブラウザ上に仮想端末が展開され、コマンドの実行がいつでも体感可能。初心者からプロまで対応する1,500以上の自己完結型ラボを提供。

1,500以上の自己完結型ラボ

Capture the Flag（CTF）

ハッカー同士が競い合うセキュリティ問題解決コンテストツール。出題された課題を先に解決した方が勝利し、ゲーミング感覚で技術習得が可能。

ゲーミング感覚で技術習得

広い実績　英国実績：警察（英国全土）・軍・防衛・大学（ウェールズ主要大学）・民間(中小〜大企業)、行政への幅

ゼロから1年で即戦力へ — 女性人材育成のロードマップ

CYBER SAMURAI PROGRAM™のロードマップ

1

今日〜1ヶ月

Basic（Level 1）

16〜20h

基礎知識を学ぶ。コンピュータの仕組み・セキュリティの概念・Linuxのコマンド操作から始める。

「なんとなくわかってきた」でOK

2

1〜3ヶ月

Essential（Level 2）

50〜54h

Kali Linuxやハッキングラボを使って実際に攻撃・防御を体験。「本物感」がまったく違う！

楽しければセンスあり！

3

3〜5ヶ月

Expert（Level 3）

30〜34h

MetasploitやNinjyaなど上級ツールを習得。SudoRangeのCTFで実戦的な腕を磨く。

ここまで来れば転職市場で通用する

4

5〜8ヶ月

Level 4（専門化）

選択制

攻撃系（CEH相当）か防御系（CISSP相当）か。自分の強みを活かして専門家へ進化。

資格取得でスキルを公式に証明

5

8ヶ月〜1年

就職・キャリア

TSL支援

セキュリティ企業・IT企業・官公庁・コンサルなど。TSLのネットワークで就職を全面サポート。

副業・フリーランスの道も！

よくいただくご質問 — 職場への案内にもお使いください

不安をすべて解消しましょう！

Q プログラミングができません…

→ OK！ Level 1はプログラミング不要でスタート。コンピュータの基礎からゆっくり学べます。A子さんもB子さんも未経験スタートでした。

Q 育児中・仕事しながらでも？

→ できます！ コホート型授業は少人数制でメンターがサポート。オンライン対応もあり。育児の合間・仕事帰りに学べる設計です。

Q 何ヶ月で仕事になりますか？

→ Basicから始めると最短8ヶ月〜1年でデビューが目安。Level 2修了後に転職活動を始めるケースも多数。副業は3〜4ヶ月から可能。

Q 本当に違法じゃないの？安全？

→ 合法です！ 演習はすべて安全な仮想環境（SudoRange）で実施。「許可を得た上で」行うのがエシカルハッカーの鉄則。倫理教育も徹底。

Q 費用はどのくらいかかりますか？

→ 詳細は個別相談で。まずは問い合わせ：y.kuwahara@trive-sl.co.jp

Q 英語が苦手でも大丈夫？

→ 全講座・サポートが日本語対応。英国発のSudoRangeも日本語でフォロー。英語力は後からついてきます！

まとめ

1. 私たちの生活はデジタル化が進み、「守るべきもの」が急増している
2. サイバー攻撃は「大企業だけの話」ではない。行政・病院・港・工場・航空が現実の標的に
3. 事故は金銭的損害だけでなく、信頼・ブランド・経営者責任にまで及ぶ
4. 日本には約40万人のセキュリティ人材が不足――今がキャリアチェンジの最大のチャンス！
5. 細やかな注意力・コミュ力・多様な視点――女性の強みがサイバーセキュリティで輝く
6. CYBER SAMURAI PROGRAM™とSudoRange™で、ゼロから1年で女性人材の即戦力化が実現できる！

Q & A

質疑応答

どんなことでもお気軽にどうぞ！

- Q　どのLevelから始めればいいですか？
- Q　育児中でも学べますか？費用は？
- Q　プログラミングが全くできなくても？
- Q　何ヶ月でLevel 1が修了できる？
- Q　CYBER SAMURAI PROGRAM™はどこで申し込める？
- Q　SudoRange™はどんな環境で学べますか？

「それなら私にもできるかも！」――ぜひTSLと連携を――貴組織の女性活躍推進に新しい選択肢を

ありがとう
ございました！

CYBER SAMURAI PROGRAM™

「それなら、うちの女性社員・受講生に紹介できるかも！！」

ぜひTSLと一緒に、次の一歩を。

桑原 義幸　（Yoshiyuki Kuwahara）

株式会社 Trive Secure Lab　執行役員副社長

y.kuwahara@trive-sl.co.jp