2025 年　10 月　現在

職務経歴書

氏名：E.K

〔 職務経歴 要約 〕

これまで、様々なプロジェクトに携わり、特にセキュリティ分野において豊富な経験を積んでまいりました。官公庁のプロジェクトでは、公的な認証基盤の設計・構築に携わり、私立大学においては、セキュリティ体制を一から構築する経験をいたしました。

その後、セキュリティコンサルタントとして様々な組織のセキュリティ課題の発見・対策、各種規程の策定や従業員へのセキュリティ啓蒙など、幅広いセキュリティ領域を担当してまいりました。

〔 職務経歴 概略 〕

1995 年 4 月 ～ 2001 年 10 月（約 6 年）ゼネコン会社にて社内システムの保守運用に従事
2001 年 11 月 ～ 2009 年 12 月（約 8 年）官公庁の電子認証局システム構築プロジェクトに参加
2010 年 2 月 ～ 2015 年 3 月（約 5 年）私立大学にて情報システム部新規立ち上げプロジェクトに参加
2015 年 4 月 ～ 2018 年 3 月（約 3 年）放送局にてセキュリティ基盤構築プロジェクトに参加
2018 年 4 月 ～ 2021 年 3 月（約 3 年）コンサルティングファームにてコンサルタントのサポートに従事
2021 年 4 月 ～ 2023 年 6 月（約 2 年）通信事業会社にて情報セキュリティマネジメント支援
2023 年 8 月 ～ 2024 年 10 月（約 1 年）広告代理店のグループ企業にてソリューション導入支援
2024 年 11 月 ～ 2025 年 9 月（約 10 ヶ月）旅行事業会社にてグループ企業のセキュリティガバナンス強化支援

〔 主な実績 〕

・セキュリティ戦略支援 / 要件整理
・情報資産のリスク評価・分析
・セキュリティ対策支援
・SOC、CSIRT 立ち上げ支援

〔 得意業務 〕

・セキュリティ戦略策定 / 運用改善
・セキュリティ課題の発見、情報収集
・セキュリティリスク評価

〔 保有資格 〕

取得年月	資格名
2016 年 1 月	ITIL V3 Foundation
2021 年 12 月	情報セキュリティマネジメント（SG）
2022 年 6 月	情報処理安全確保支援士(SC)
2023 年 1 月	公認情報セキュリティマネージャー（CISM）
2024 年 4 月	セキュリティ プロフェッショナル認定資格制度（CISSP）

〔 職務経歴詳細 〕

期間	プロジェクト名と業務内容	利用技術	役割 /案件規模
2024 年 11 月 ～ 2025 年 9 月 （10 ヶ月間）	旅行事業会社/ セキュリティガバナンス強化 【プロジェクト概要】 グループ企業のセキュリティガバナンス強化のため、各事業会社のセキュリティ課題の洗出しと対策支援を行う 【担当業務】 ■ セキュリティ戦略支援 ■ セキュリティリスク評価 ■ セキュリティ対策支援 ■ 規定類の見直しと策定 ■ セキュリティ担当者育成支援	【セキュリティフレーム】 ・サイバーセキュリティ経営ガイドライン ・政府統一基準群 ・NIST-SP-800-171 ・CIS Controls	役割： コンサルタント 従業員数: 【単体】約 160 名 【グループ】 約 2750 名 グループ企業： 16 社
	【主な実績・取り組み】 アサイン後、セキュリティ担当の社員を手配できず、セキュリティ推進を一人で行っておりました。 しかし、次のフェーズの CSIRT 設置に向けて準備を進めていましたが、予算の都合によりプロジェクトは終了となりました。		
期間	プロジェクト名と業務内容	利用技術	役割 /案件規模
2023 年 8 月 ～ 2024 年 10 月 （1 年 3 ヶ月間）	広告代理店 / 情報セキュリティマネジメント支援 【プロジェクト概要】 全グループ企業に CNAPP の導入支援を行う。 【担当業務】 ■ 情報セキュリティ要件整理 ■ ソリューション選定支援 ■ 運用設計 ■ グループ企業向け説明資料作成 ■ グループ企業へ提案交渉 ■ グループ企業へソリューション導入支援	【セキュリティソリューション】 ・Cloudbase	役割：メンバー メンバー数：6 名 従業員数: 【単体】約 5200 名 【グループ】 約 2750 名 グループ企業： 32 社
	【主な実績・取り組み】 グループ企業毎の資産情報の棚卸しから、運用設計まで行う　2023 年 8 月-2024 年 7 月 CNAPP を導入するために、各グループ企業のシステム構成から情報資産の棚卸しまでを支援する。また、組織ごとのリソースや組織文化などを考慮して運用設計を行う。		

期間	プロジェクト名と業務内容	利用技術	役割 /案件規模
2021 年 4 月 ～ 2023 年 6 月 （2 年 3 ヶ月間）	通信事業会社 / 情報セキュリティマネジメント支援 【プロジェクト概要】 社内の情報セキュリティマネジメントの支援を行う。情報資産の棚卸しからセキュリティ体制の現状把握、リスクアセスメント、対策検討・提案、教育・訓練の実施などを行う。 【担当業務】 ■　情報セキュリティ戦略支援 ■　セキュリティレベルの向上や改善提案 ■　セキュリティリスクアセスメント ■　セキュリティポリシーなどの規定類の作成支援 ■　セキュリティ業務フロー作成支援 ■　セキュリティ研修支援	【セキュリティフレーム】 ・サイバーセキュリティ経営ガイドライン ・NIST SP 800-53 ・CIS Controls	役割： 運用設計担当 メンバー数：6 名 従業員数: 【単体】約 7 千名 【連結】約 2 万名 売上高: 約 2 千億円
	【主な実績・取り組み】 陳腐化したセキュリティポリシーなどのドキュメントを刷新　2018 年 7 月-2020 年 4 月 作成した文章を改定することに抵抗を感じる社内文化が根強く 5 年も、10 年も前に作成されたままのセキュリティポリシーや基本方針などのドキュメントがそのままとなっていた。経営層を巻き込みながら、最新のセキュリティ環境やトレンドと組織戦略を考慮して定期的な見直しを行うフローを提案し具体的なプロセスを策定、実施を行う。 従業員のセキュリティ理解度とエンゲージメントを向上　2018 年 10 月-2020 年 3 月 複雑で難解な専門用語を使用することなく、リスクシナリオをもとにリスクアセスメントレポートやセキュリティトレーニングを提供することで、従業員の理解度とエンゲージメントを向上させた。		

2021 年 4 月　～　2023 年 6 月　通信事業会社での主な担当プロジェクト

期間	プロジェクト内容	役割／環境	実績／ポイント
2021 年 6 月 ～ 2022 年 3 月	■ Microsoft Intune の運用設計 以下の運用設計を行う 「デバイス管理」 「アプリケーション管理」 「コンプライアンス ポリシー管理」 「更新プログラム管理」「脆弱性管理」 【担当】 ・運用設計　・進捗管理 ・ベンダー折衝　・部署間調整	【役割】 ・運用設計担当者 【セキュリティソリューション】 ・Microsoft Intune ・Microsoft Defender For Endpoint	ベンダーと協力しながら、何ができるのかを検討し、できるだけ利用者の利便性を損なわないように運用設計を整備しました。
2021 年 12 月 ～ 2023 年 6 月	■ リスクアセスメント 社内で利用するシステム、社外に提供するシステムのリスクアセスメントの業務フローの設計構築、運用まで行う 【担当】 ・セキュリティリスクアセスメント	【役割】 ・運用設計担当者 ・アセスメント実施者 ・PMO [プロジェクト要員] メンバー：5 名	リスクアセスメントを実施していなかったため、現在使用しているシステムも含めてアセスメントを実施。 それに合わせて、アセスメントフローを設計する。 アセスメント結果によりリスク対応支援まで行う。 申請件数が多くなり、PMO として進捗管理や調整、課題管理なども行う。
2022 年 3 月 ～ 2022 年 10 月	■ セキュリティ教育・啓発 e-Learning だけでなく、講習会などを開きセキュリティ教育や啓発活動を行う 【担当】 ・セキュリティ研修のコンテンツ作成	【役割】 ・講習会講師	e-Learning では、社内ポリシーなどの規定類を中心とした研修を行い、講習会では、役職や部署ごとにそれぞれの業務内容に即した研修を行っておりました。 研修後は、参加者同士でディスカッションをして頂き、内容を発表していました。 また実際に、Wireshark でパケットを解析し平文の通信内容を見せたり、フィッシングサイトを作成しパスワードを入手したり、簡易的なハッキングの実演は評判が良かったです。
2021 年 10 月 ～ 2023 年 4 月	■ 組織横断型の CSIRT 立ち上げ支援 インシデントレベルや連絡体制など各部署と調整を行いながら構築支援を行う 【担当】 ・セキュリティ運用設計支援	【役割】 ・運用設計	シナリオを元にインシデント訓練を行う。 インシデントの検知から、封じ込め、駆除、原因と対策まで訓練として行う。 また、訓練のふり返り行い問題点を洗い出し体制強化を行う。

<table>
<tr><th>期間</th><th>プロジェクト名と業務内容</th><th>利用技術</th><th>役割 /案件規模</th></tr>
<tr><td>2018 年 4 月
～
2021 年 3 月

（約 3 年）</td><td>コンサルティングファーム /
セキュリティコンサルティングのアシスタント

【プロジェクト概要】
セキュリティコンサルティングのアシスタントとして、セキュリティ支援を行う。

【担当業務】
■ 情報セキュリティに関する課題の抽出
■ セキュリティポリシーの策定支援
■ セキュリティ設計支援
■ セキュリティ運用設計
■ セキュリティリスクアセスメント
■ セキュリティ対応、対策支援</td><td>【セキュリティフレーム】

・サイバーセキュリティ経営ガイドライン

・NIST SP 800-53

・CIS Controls

・COBIT-2019</td><td>役割：
アシスタント

メンバー数：
17 名</td></tr>
<tr><td></td><td colspan="3">【主な実績・取り組み】
セキュリティコンサルティングのアシスタント 2018 年 4 月-2021 年 3 月
コンサルタントのアシスタントとして、様々な組織のセキュリティ課題を調査し、対策の提案から構築、運用まで幅広く支援を行う。</td></tr>
</table>

2018 年 4 月　～　2021 年 3 月　コンサルティングファームでの主な担当プロジェクト

期間	プロジェクト内容	役割／環境	実績／ポイント
2018 年 4 月 ～ 2019 年 3 月	医療関連事業会社/ リモート医事事務サービスのセキュリティ リモートで医療事務業務を行うシステム設計から運用業務プロセスの構築まで幅広くセキュリティ対策を行う 【担当】 ・セキュリティア設計支援	【役割】 ・コンサルティング [プロジェクト要員] お客様担当者：15 名 コンサルタント：5 名	3 省 2 ガイドラインに従ったセキュリティプランの提案や、「匿名加工医療情報」など患者情報の取扱いなどの提案を行う。
2019 年 10 月 ～ 2020 年 6 月	ビルメンテナンス会社 / 再生可能エネルギーの最適化システム 再エネを最適化するシステムの企画段階から参画し、よりセキュアなシステム開発を行う 【担当】 ・セキュリティリスクアセスメント	【役割】 ・コンサルティング [プロジェクト要員] お客様担当者：5 名 コンサルタント：3 名	企画・設計の段階からセキュリティ要件を取り込んだシステム開発を行うことができた。
2020 年 4 月 ～ 2020 年 10 月	林業事業会社 / 情報セキュリティ体制の強化支援 セキュリテチーム体制や業務プロセスなどの改善提案を行う 【担当】 ・セキュリティ設計支援	【役割】 ・コンサルティング [プロジェクト要員] お客様担当者：7 名 コンサルタント：2 名	現状分析から課題の発見と対策提案を行う。 セキュリティポリシーやインシデント対策、情報資産管理など整備を行う。
2020 年 6 月 ～ 2020 年 12 月	人材派遣会社 / SOC の立ち上げ支援 NTTCom「WideAngle」サービス導入支援とそれに伴う SOC チームの立ち上げ支援を行う 【担当】 ・セキュリティ運用設計支援	【役割】 ・コンサルティング [プロジェクト要員] お客様担当者：3 名 コンサルタント：2 名	解析用ログ管理から構成管理、アラート通知後のフロー策定などの支援を行う。
2020 年 11 月 ～ 2021 年 3 月	特許事務所 / 情報セキュリティアセスメント調査 お客様先の情報セキュリティアセスメントプログラムの構築支援を行う 【担当】 ・セキュリティ運用設計支援	【役割】 ・コンサルティング [プロジェクト要員] お客様担当者：9 名 コンサルタント：1 名	「現用調査」「リスク分析」「対策立案」「対応計画」等の各プロセスフローをお客様とともに構築を行う。

期間	プロジェクト名と業務内容	利用技術	役割 /案件規模
2015 年 4 月 ～ 2018 年 3 月 （約 3 年）	放送局 / サプライチェーン攻撃対策の セキュリティ基盤構築 【プロジェクト概要】 サプライチェーン攻撃の対策として 放送局並びに関連団体の不正通信を 監視するセキュリティ基盤の構築 【担当業務】 ■ 各関連団体への提案交渉 ■ 関連団体向け説明資料作成 ■ 各関連団体のネットワーク構成調査 ■ Active Directory ポリシー設計 ■ 各関連団体の Firewall ルール作成 ■ ベンダー折衝 ■ セキュリティ基盤設計支援 ■ Tanium / Splunk 構築支援 ■ 地方放送局のネットワーク構成調査、 基盤受け入れフロー、手順書作成 ■ 運用定義書作成	【サーバ】 ・VMware ESXi ・WindowsServe2016 ・RedHat 【ネットワーク】 ・Palo Alto 【セキュリティ ソリューション】 ・Tanium ・Splunk 【言語】 ・Python	役割： ・運用設計 SE ・SOC マネジメント メンバー数：9 名 [プロジェクト要員] ・放送局員 5 名 ・コンサルタント 8 名 [外部ベンダー] ・セキュリティ基盤 ・SOC ・Tanium / Splunk ・利用申請システム ・構成管理システム [利用者] ・関連団体数 27 団体 ユーザー数 約 8 万人 ・放送局独自回線数 約 3 万回線
	【主な実績・取り組み】 セキュリティ基盤運用マネージャー 2016 年 2 月-2018 年 3 月 新規運用チームの立ち上げからマネジメントまで行う。また、お客様の Firewall ルール作成やセキュリティソリューションなどのご相談に対応し、お客様から感謝状を表彰される。 運用設計担当者 2015 年 6 月-2017 年 3 月 提案交渉から参加することで、ベンダーと調整を行いながら運用設計をすることができた。その結果、効率的な運用やお客様サポートを充実させることができた。 提案交渉 2015 年 4 月-2015 年 12 月 交渉時にプロジェクト参加を勧めると共に、「セキュリティ情報の共有」「団体毎のセキュリティソリューションの提案」「インシデント対応以外のセキュリティ対応」などを提案することで、短期間で 27 団体と合意形成が出来、信頼関係を構築することができた。		

2015 年 4 月　～　2018 年 3 月　放送局での主な担当プロジェクト

期間	プロジェクト内容	役割／環境	実績／ポイント
2015 年 5 月 ～ 2016 年 3 月	■関連団体提案交渉 / 構成調査 不正アクセスによる情報漏洩リスクの対応として、不正通信を監視しするプロジェクトへの理解と参加を提案交渉する また、それに伴いネットワーク構成の調査を実施 【担当】 ・運用設計	【役割】 ・運用設計担当者 [プロジェクト要員] 放送局員：2 名 コンサルタント：2 名	現状で問題が起きていないセキュリティ対策に対して、新たに通信の監視やネットワーク構成の変更、それに伴う費用負担を求める厳しい交渉を行いました。 ・セキュリティ情報の共有 ・新たなセキュリティソリューション ・インシデント対応以外の対応 など運用設計として付加価値を提案することで理解をして頂くことができました。
2015 年 10 月 ～ 2016 年 3 月	■セキュリティ基盤構築 不正通信を監視するために通信経路を集約するための基盤構築 【担当】 ・運用設計　・進捗管理 ・ベンダー折衝　・部署間調整	【役割】 ・運用設計担当者 [プロジェクト要員] 放送局員：2 名 コンサルタント：2 名 【ネットワーク】 Palo Alto / Cisco 【仮想環境】 VMware ESXi	「SOC（Tanium / Splunk)」の基盤構築を行いました。 また、基盤に引き入れるために、関連団体の構成調査などを行い、基盤に集約しました。
2016 年 1 月 ～ 2016 年 7 月	■Tanium / Splunk 構築 「Tanium」：不正通信を行っている端末をネットワークから隔離する 「Splunk」：端末情報ログや通信ログを収集し、「端末調査」「ネットワーク調査」を行う 【担当】 ・PM　・ベンダー折衝 ・運用設計	【役割】 ・PM ・運用設計担当者 [プロジェクト要員] 放送局員：2 名 コンサルタント：2 名 【仮想環境】 VMware ESXi 【言語】 Python	Splunk に収集している通信ログから脅威ログを検索、その結果から Tanium で不正通信を行っている端末を特定、ネットワークからの隔離を自動で行うためのスクリプトを Python で作成しました。 その結果、運用員負担の軽減やオペレーションミスを防止することができました。
2016 年 1 月 ～ 2016 年 5 月	■Active Directory 構築 関連団体に Active Directory を構築し、ベースポリシの設計を行う 【担当】 ・運用設計　・ベンダー折衝	【役割】 ・運用設計担当者 [プロジェクト要員] 放送局員：2 名 コンサルタント：2 名 【サーバ】 WindowsServe2016	放送局、関連団体における基礎ベースとなるグループポリシーの設計を行いました。
2016 年 2 月 ～ 2018 年 3 月	■運用マネジメント 新規運用チームを立ち上げ、運用員のマネジメントを行う 【担当】 ・運用定義　・運用体制構築 ・ナレッジ管理　・運用員人材育成	【役割】 マネージャー メンバー数：9 名	ワークフロー、手順書に従って運用、保守を行うだけでなく自ら提案して改善を行うチーム作りをしています。 作業スペースにホワイトボードを設置し、問題や改善点を付箋でいつでも記入できるようにし、解決すると付箋を外すようにしています。 目に入るところにホワイトボードを置くことで常に、問題意識を持ちながら作業を行うことができるようになりました。

<table>
<tr><th>期間</th><th>プロジェクト名と業務内容</th><th>利用技術</th><th>役割 /案件規模</th></tr>
<tr><td>2010 年 2 月
～
2015 年 3 月

（5 年 2 ヶ月間）</td><td>私立大学 / 情報システム部新規立上げ

【プロジェクト概要】
新規情報システム部立上げとともに ICT 環境整備を実施

【担当業務】
■ システム刷新、新規導入
■ ネットワーク / サーバ
設計・構築・運用・管理
■ 情報セキュリティ対策
・学内セキュリティポリシーの草案作成
・情報資産の棚卸し
・業務フローの見直し
・インシデント対策
・リスク分析とシナリオ作成
・セキュリティ研修
■ Active Directory 設計・管理
■ 障害対応（検知～復旧、
原因分析、再発防止策実施）
■ 主に ACCESS や EXCEL での
業務支援アプリケーションを VBA で開発</td><td>【サーバ】
・Linux 約 20 台
・WindowsServe
2008R2 約 4 台
・Windows 7
約 1000 台

【DB】
・Oracle
・MySQL

【仮想環境】
・VMware ESXi

【監視ツール】
・WhatsUp Gold
（ネットワーク監視）

・Nagios
（システム監視）</td><td>役割：
・リーダー
・PM
・PMO
メンバー数：6 名

ユーザー規模
学生 約 6000 名
教員 約 700 名
職員 約 300 名</td></tr>
<tr><td></td><td colspan="3">【主な実績・取り組み】
スキルアップ研修 リーダー 2010年2月-2015年3月
経験もスキルもバラバラな職員に対し、ITスキルの底上げだけでなくヒアリングや要件定義などのプロジェクトの進め方などを教育する。その結果、主体的に提案やプロジェクト管理を行えるようになる。

インフラ整備・システム群の最適化 2010年5月-2015年3月
システム障害や、通信障害が頻発するネットワークなど学内のボルトネックを見つけ出しグラウンドデザインから見直しを行い、最適化を行う。

情報処理委員会の設立 2010年5月-2010年9月
学内の経営層や教職員で構成した「情報処理委員会」を新規に設立し、学内の IT 戦略について意思決定を行う。教員や職員、経営層など様々な立場のユーザーに対して統一の目的や危機感を共有することで、問題解決が迅速に行えるようになる。</td></tr>
</table>

2010 年 2 月　～　2015 年 3 月　私立大学での主な担当プロジェクト

期間	プロジェクト内容	役割／環境	実績／ポイント
2010 年 4 月 ～ 2011 年 3 月	■学内ネットワークの再構築 学内の VLAN/PVLAN/ACL/PortSecurity などの設計から導入をベンダーとともに行う 【担当】 ・ネットワーク要件定義　・部署間調整、 ・構成設計、　・運用設計 ・ベンダー折衝　・コスト管理 ・進捗管理	【役割】 ・PM メンバー数：3 名 【L3 スイッチ】 Catalyst - 3750 シリーズ 【L2 スイッチ】 Catalyst - 2960 シリーズ	トラフィック調査を行い、VLAN 設計の見直しを提案し、実施しました。 設定変更後、エンドユーザからネットワークフォルダへのアクセスやインターネット使用時に体感速度が劇的に改善されたと評価を頂きました。
2010 年 9 月 ～ 2011 年 3 月	■ActiveDirectory の再構築 WindowsServe2003 から 2008R2 にリプレイス作業を実施。OU 再設計、GPO 再設定を行う 【担当】 ・現状分析　・進捗管理 ・新業務フローの考案　・部署間調整 ・要件定義　・セキュリティポリシーの策定	【役割】 ・PM メンバー数：2 名 【サーバ】 WindowsServe 2008R2 （DC） 約 4 台 【クライアント】 Windows 7 約 1000 台	職員、教員、学生や非常勤、院生などの異なる属性アカウントのアクセス制限を見直し、職員ドメイン、学生ドメインに再構築する。 証明書やグループポリシーで、 セキュリティ対策を行うとともに、 シングルサイオンで利便性も向上することができました。
2011 年 4 月 ～ 2011 年 12 月	■e ラーニングシステムの構築～運用 OSS の e ラーニングシステムを Linux にて設計から構築、運用保守を行う 【担当】 ・要件定義　・設計 ・構築　・各種ドキュメント作成 ・運用　・新業務フローの考案 ・部署間調整	【役割】 ・PMO メンバー数：2 名 【仮想環境】 VMware ESXi [仮想マシン] Linux　2 台 【DB】 MySQL　2 台	学業とコンピュータシステムとの融合を理念として e ラーニングシステム（Moodle/Mahara)の構築を行いました。 AP 層(2 台)とディレクトリ・DB 層(2 台)の 2 層構造にして高可用性とアクセスの負荷分散構成で構築しました。 より充実した学習環境を提供するため、教員と共にコンテンツ作成が非常に苦労致しました。
2013 年 5 月 ～ 2013 年 12 月	■研究業績データベースシステム導入 各教員の様々な情報（プロフィール、研究業績など）を登録・管理するシステムの導入 【担当】 ・要件定義　・新業務フローの考案 ・システム環境選定・ベンダー折衝 ・基本設計　・外部交渉進捗管理 ・部署間調整	【役割】 ・PMO メンバー数：2 名 【仮想環境】 VMware ESXi [仮想マシン] Linux　2 台 【外部サービス】 ReaD&Researchmap	5 つの部署が使用するシステム導入のため各部署の業務内容と要望を取りまとめ 予算内に機能を実装するため、ベンダーとの交渉を粘り強く行った結果、要件通りのシステムを予算内で導入することができました。その後ベンダーと良好な関係を築き、拡張機能や改修など建設的なシステム運用を行う事が出来ました。
主な 開発システム	□業務支援システム開発 ・ヘルプサポート/障害管理システム ・パスワード管理システム ・ファイルサーバのログ解析、集計報告書システム ・入学者管理システム ・会議室予約管理システム	【役割】 開発者：1 名 【ツール】 MS-ACCESS 【言語】　VBA SQL	各部署とのコミュニケーションから 支援システムを開発してきました。 主に MS-ACCESS や EXCEL での開発が多いですが、教職員用に Moodle システムを構築し、アンケートや掲示板など業務に利用できるようなモジュールを使用して業務支援を行いました。

期間	プロジェクト名と業務内容	利用技術	役割 /案件規模
2001 年 11 月 ～ 2009 年 12 月 （8 年 2 ヶ月間）	官公庁 / 電子認証局システム 【プロジェクト概要】 認証基盤システムの運用設計から運用マネジメントまで行う 【担当業務】 ■ データセンター全体運営 ■ 運用マネジメント ■ 情報セキュリティ対策 ■ 証明書の発行、登録 ■ 障害対応 ■ ベンダー折衝	【サーバ】 ・UNIX (Solaris) 約 100 台 ・WindowsServe2003 約 10 台 【DB】 ・Oracle 【監視ツール】 ・JP1 （Job 監視、 ネットワーク監視） ・Tripwire （システム監視）	役割： ・設計・構築 SE ・運用マネジメント
	【主な実績・取り組み】 運用員にマニュアルや手順書通りにただ行わせるのではなく、なぜその作業が必要なのかを考え、理解させながら作業を行わせる。その結果、運用員によるヒヤリ・ハットやヒューマンエラーが減少し、システムの安定稼動につながる。		

期間	プロジェクト名と業務内容	利用技術	役割 /案件規模
1995 年 4 月 ～ 2001 年 10 月 （6 年 7 ヶ月間）	大手ゼネコン企業 ／ 社内システム 【プロジェクト概要】 社内システムの保守運用を担当 【担当業務】 ■ PC 管理・ライセンス管理、ヘルプデスク対応 ■ Windows・UNIX サーバの保守、運用 ■ Oracle データベースの保守、運用	【サーバ】 ・UNIX(HP) 約 200 台 ・Windows2000 Server 約 20 台 【DB】 ・Oracle	役割：メンバー メンバー数：8 名
	【主な実績・取り組み】 月次の集計レポートを自動集計するツールを VBA で開発 社員 2 名で作成している集計レポートを数秒で作成が出来ると、評価をいただく。 このとこがきっかけで IT の職業に興味を持つようになる。		

〔 自己 PR 〕

情報セキュリティをマネジメントすることができる

これまで、さまざまな企業でセキュリティ対策に携わってきました。
セキュリティ対策は、組織の目的や目標を達成するために必要不可欠なものだと考えています。
セキュリティソリューションの導入や、教育・啓発などの個別対策だけでなく、企業全体のセキュリティリスクを視野に入れた、統合的なセキュリティのマネジメントを行う必要があると考えております。
私は、これまでに組織のガバナンス強化として、セキュリティ戦略や対策の設計と実装を行ってきました。

常に学び続け、組織に貢献することができる

「情報処理安全確保支援士」をはじめとする国内外のセキュリティ資格を取得し、資格維持のために年 10 回以上のセミナーや研修に参加し、最新のセキュリティ技術に関する知識をアップデートしています。
最新の技術動向をキャッチアップし業務に活かすことで、組織へ貢献することができます。

目的を見失わないセキュリティ対策を行うことができる

セキュリティ対策は、あくまでもビジネス目標を達成するための手段の一つに過ぎません。
しかし、さまざまな企業のセキュリティ対策を見てきましたが、その中で手段が目的化しているケースが多数ありました。
例えば、フィッシングメール訓練において、従業員がフィッシングメールを開封すると情報システム部へ連絡させ、開封率を公開し注意喚起を行う、といったケースです。
本来の目的である「フィッシングメールに適切に対応できる能力を身につける」ことより、「フィッシングメールを開封しない」ことが目的となっているケースがあります。
フィッシングメール訓練では、開封後のフローが重要であり、平時に作成したインシデント対応マニュアルが機能するかを検証し、各担当者が適切に対応できるようにする必要があります。
私は以前、通信事業会社でフィッシングメール訓練ではなく、様々なシナリオに基づいたインシデント訓練を実施しました。この方法では、従業員は実際のインシデント発生時と同様の状況を体験し、マニュアルに沿って対応することで、より実践的なスキルを習得することができます。
この取り組みを通じて、目的と手段を混同することなく、より効果的なセキュリティ対策を実現することができました。
セキュリティ対策は、あくまでも手段です。その目的を見失わず、ビジネス目標達成に貢献するようなセキュリティ対策を行うことができます。

以上