

職務経歴書

平成 XX 年 X 月 XX 日
氏名：XXXXXXXX

専門業務分野

- 企業、官公庁向けセキュリティコンサルティング業務
 - ・ セキュリティホール調査（ペネトレーションテスト）、不正アクセス被害調査
 - ・ 個人情報流出経路の特定など

専門技術分野

- Linux、Windows、UNIX、Cisco ルータなどのサーバ、ネットワーク機器に対するセキュリティホール調査（年間約 30 社程度）の計画立案、実施、報告、改善提案を担当。
- 不正アクセスの被害を受けたサーバの侵入経路、被害状況の調査・再現・報告や関係者へのヒアリングなどを担当。

Point 1

今までの業務経験の詳細を記してから、提案、マネジメントを活かす経験を伝える。

自己PR

- 現在の部署に配属されてから約 4 年間、主にセキュリティホール調査という業務を通じて企業や官公庁の情報セキュリティの現状に触れ、問題点の指摘、改善策の提案を行って参りました。
- 上記以外にも業務で得た知識を基に「ネットワークセキュリティ」に関するセミナー講師や雑誌の執筆を担当しました。
- これまでの業務では情報セキュリティの技術的側面と向きあうことが多かったのですが、より正確なリスクアセスメントを行うために情報セキュリティ全般のマネジメントに携わり、顧客の要望に適したソリューションを提案したいと考えております。

また、今後普及を予想する情報セキュリティ監査の監査人を目指し、組織の情報セキュリティマネジメントの支援を行いたいと考えております。

職務経歴

株式会社++++ (20XX/04 ~ 20XX/04)

開始時期	内 容
20XX 年 4 月 ~ 20XX 年 X 月	事業本部 <担当業務> 内部監査支援 <担当役割> セキュリティエンジニア <PJ 規模> 5 名 <技術要素・環境> 大手通信会社で実施された内部監査を技術的側面から支援。 被監査部門とのスケジュール調整、Windows/Linux/UNIX サーバに対するセキュリティ調査、監査報告書作成支援を担当。
20XX 年 2 月 ~20XX 年 3 月	事業本部 <担当業務> 不正アクセス被害調査 <担当役割> セキュリティエンジニア <PJ 規模> 2 名 <技術要素・環境> 某信販会社が利用していたサーバが不正アクセスを受けたため、その侵入経路、被害状況の調査を実施。データベースで個人情報を管理していたため、情報漏えいの可能性の有無も調査。被害状況を取りまとめ、関係者各位に報告会を実施。

Point 2

対応先と役割の詳細を記すことにより、セキュリティ製品の支援ではなく、内部監査としての役割でセキュリティコンサルを行った経験を PR できている。

<p>20XX年1月 ~20XX年2月</p>	<p>事業本部 <担当業務> 個人情報漏洩事件に関する調査 <担当役割> セキュリティエンジニア <PJ規模> 5名 <技術要素・環境> 大手通信会社の個人情報漏洩事件の発端となったデータベースサーバに対し、セキュリティホール調査を実施。情報の流出経路が存在するかを確認し、発見された問題点に対して改善策を提案。</p>
<p>20XX年12月</p>	<p>事業本部 <担当業務> 某官公庁の電子申請システムに対するセキュリティ監査 <担当役割> セキュリティエンジニア <PJ規模> 5名 <技術要素・環境> 運用開始前の電子申請システムに対してセキュリティ監査を実施。 セキュリティホール調査やサーバ設定状況のチェックを行い、実施すべき改善策を提案。</p>
<p>20XX年6月 ~20XX年10月</p>	<p>事業本部 <担当業務> ネットワークセキュリティに関するセミナー講師 <担当役割> セミナー講師 <PJ規模> 2名 <技術要素・環境> 高度ポリテクセンターにてネットワークセキュリティに関する講師を担当。当時話題になったワームの解説やクラッカーの手口などの実演を行い、ネットワーク犯罪が身近なものであることを伝え、セキュリティ対策の必要性を説明。</p>
<p>20XX年3月 ~20XX年4月</p>	<p>事業本部 <担当業務> 大手自動車会社に対するセキュリティコンサルティング <担当役割> セキュリティエンジニア <PJ規模> 6名 <技術要素・環境> 国内・海外のグループ会社と共同で使用する、社内システムのセキュリティレベルを維持するためのコンサルティング業務。</p>
<p>20XX年10月 ~20XX年12月</p>	<p>事業本部 <担当業務> 内部監査支援 <担当役割> セキュリティエンジニア <PJ規模> 6名 <技術要素・環境> 某銀行で実施された内部監査を技術的側面から支援。被監査部門とのスケジュール調整、Windows/Linux/UNIXサーバに対するセキュリティ調査、内部監査室への報告を担当。</p>

20XX年6月 ~20XX年9月	現状把握/構築要件確認/定期診断などの目的を持った企業、官公庁のネットワークに対するペネトレーションテストを担当。 <u>(年間20~30案件)</u> Internet Scanner (ISS社製)、Nessusといったセキュリティホール調査ツール等を使用し、UNIX、Windows、Linuxなどのサーバ機器に対してテストを実施。 <u>結果解析、報告書作成の後、顧客(エグゼクティブ層、エンジニア)に対して報告会を実施。</u> 20XX年6月~20XX年3月はOJT期間
---------------------	--

以上

Point 3

対応顧客のポジションを記すことで、対応してきた責任感と、提案書・報告書のレベルが高いことがうかがえる。

書類選考通過への 重要 Point !

自己PRの簡略な詳細表現と、経歴詳細を直近の勤務から表記している点が重要。その中でも、専門用語を巧みに表記し、セキュリティエンジニア~コンサルタント職としてのキャリアアップを表現していることが注目ポイントです。
セキュリティ業界経験者は、是非参考にしてみてください。