調査研究部会

X.1060マップ活用WG 始動報告

※2025年6月より活動開始した為、開始報告となります

2025年7月23日

WGリーダー：小坂 和哉（株式会社NTTデータ）

自己紹介

- 名前：小坂 和哉
- 資格：CISSP,CCSP
- 所属：株式会社NTTデータ
- 業務：IT/OT(工場・ビル等)セキュリティ対策SI
  社内 技術勉強会の講師・運営

なぜX.1060に着目したか

お客様

セキュリティ対策や運用ってどこがゴールですか？
何かいいチェックリストはないですか？
網羅的で完璧なセキュリティ対策がしたいです

国際機関などが出しているフレームワークを活用すると
網羅的に書いてありますよ。X.1060とかどうでしょう。

セキュリティSI屋
NTTデータ 小坂

具体的なこと書いてなくて余計分からなくなりました。。
例えばX.1060ならNTTデータはどこまでサポート出来ますか？

NTTデータは多くの項目でサポート可能です。
確かに抽象的で難しい部分もありますね。
サービスマップを作った方がいいですか？

イイですね！欲しいです。期待しいてます。
ついでに他社の情報もあると便利です。

X.1060とは

X.1060とは

ITU-T勧告 X.1060は、サイバーリスク対応のための組織のフレームワークを定義した国際勧告です。

ISOG-J WG6の「セキュリティ対応組織の教科書」※が元になっています。

「組織において、ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体」としてのサイバーディフェンスセンター(CDC)を構築しマネジメントするためのフレームワークが記載されています。

※ISOG-J：セキュリティ対応組織の教科書
https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html

セキュリティ対応組織の教科書
CDCを構築・マネジメントするには

CDCを構築・マネジメントするには

CDCの運営における関係者とその役割

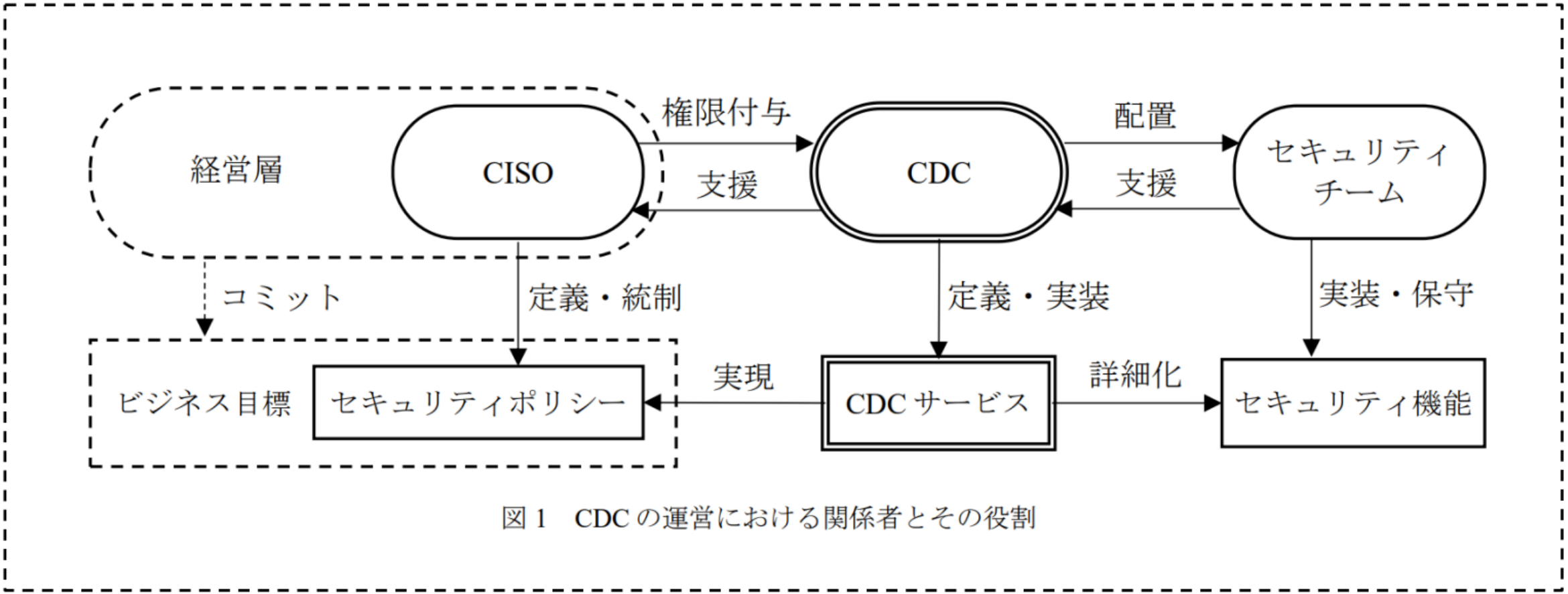

図 1　CDC の運営における関係者とその役割

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

構築・運用のフレームワーク

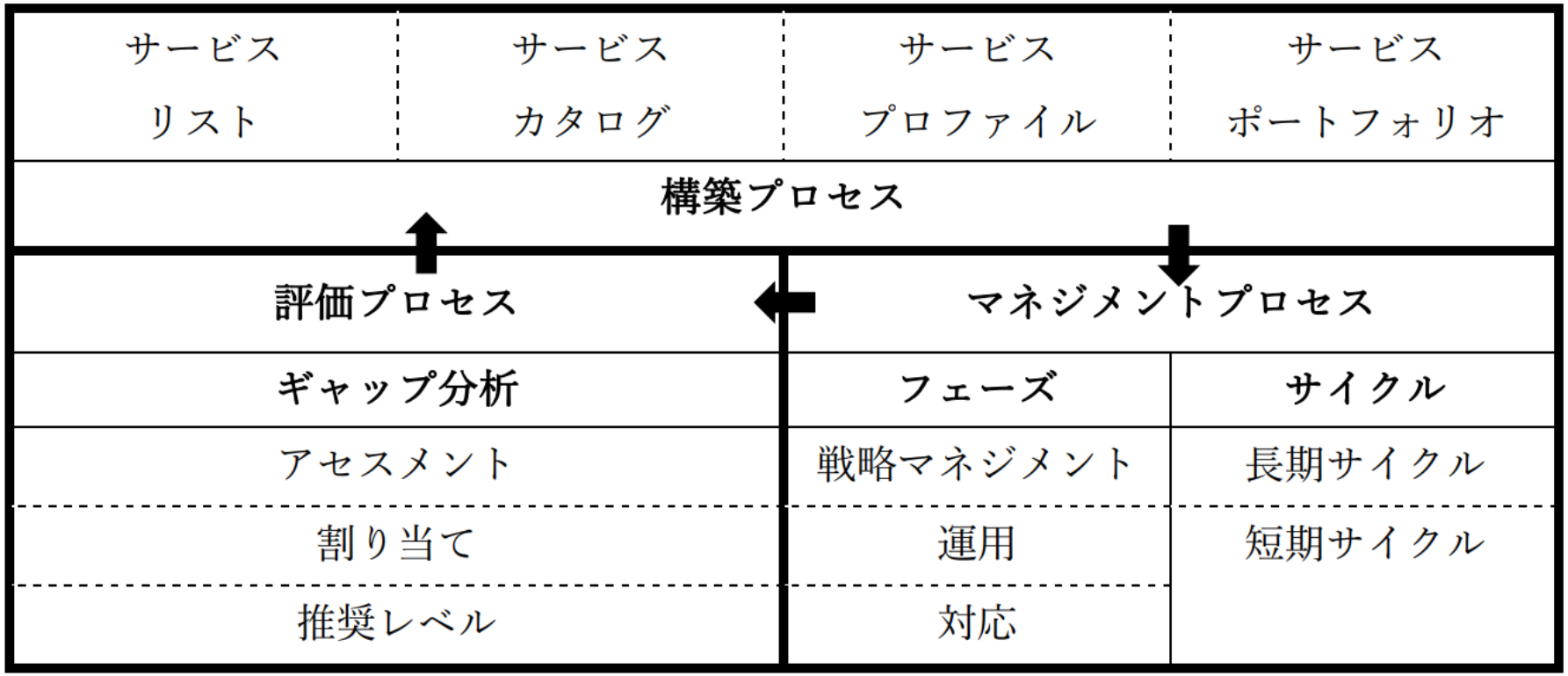

図 8 サイバーディフェンスセンターを構築・運用するためのフレームワーク[12]

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

セキュリティ対応実行サイクル

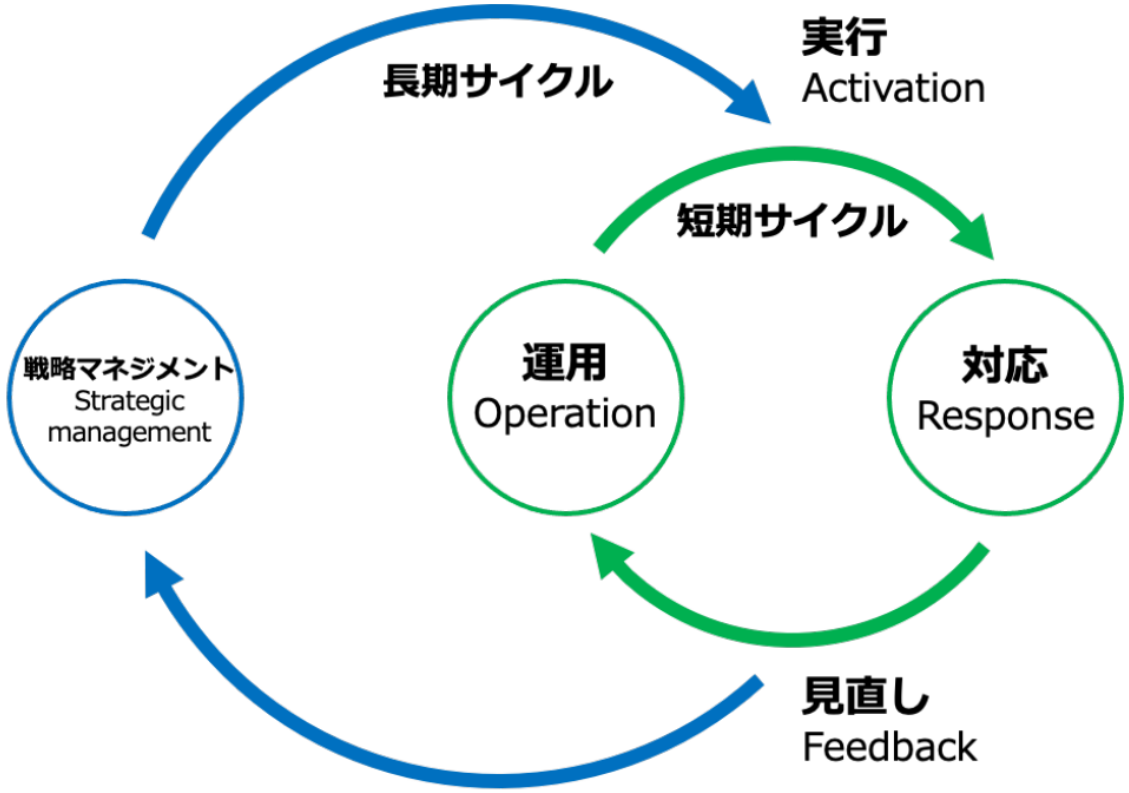

図 11 セキュリティ対応実行サイクル

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

カテゴリー

表 6 X.1060/JT-X1060 のカテゴリー

カテゴリー
A. CDC の戦略マネジメント
B. 即時分析
C. 深掘分析
D. インシデント対応
E. 診断と評価
F. 脅威情報の収集および分析と評価
G. CDC プラットフォームの開発・保守
H. 内部不正対応支援
I. 外部組織との積極的連携

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

カテゴリーと実行サイクル

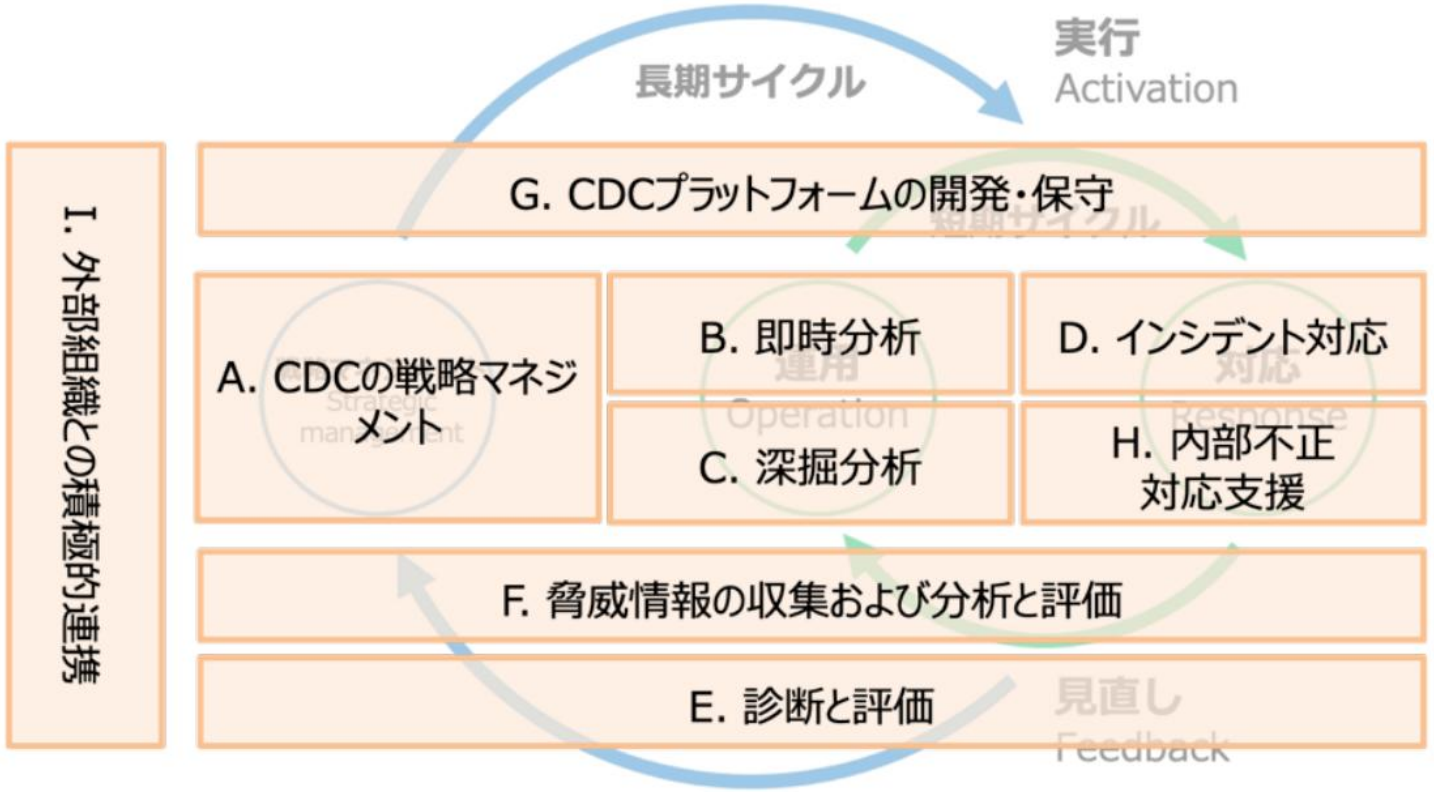

図 13 カテゴリーと実行サイクル

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

9カテゴリー・合計64個のサービス

カテゴリー	サービス
D. インシデント対応	D-1. インシデント報告受付 D-2. インシデントハンドリング D-3. インシデント分類 D-4. インシデント対応・封じ込め D-5. インシデント復旧 D-6. インシデント通知 D-7. インシデント対応報告
E. 診断と評価	E-1. ネットワーク情報収集 E-2. 資産棚卸 E-3. 脆弱性診断 E-4. パッチ管理

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

サービスの説明

E-3. 脆弱性診断

X.1060/JT-X1060 での概要は以下である。

「脆弱性診断」サービスは、ネットワーク、システム、アプリケーションの脆弱性を特定し、その脆弱性がどのように悪用されるか判断するとともに、リスクをどのように軽減できるかの提案を実現する。

守るべきシステムやネットワーク、アプリケーションに脆弱性が無いかをツールを使って確認する。プラットフォーム診断、Web アプリケーション診断、Web API 診断、スマートフォンアプリケーション診断など、目的に合わせた診断の種類を選択する。ツールでの確認であるため、精度の問題はあるものの、低コストかつ短期間で実施できるため、より多くのシステムに対する定期的な診断も行う。

出典:セキュリティ対応組織の教科書第3.2版

CDCを構築・マネジメントするには

X.1060/セキュリティ対応組織の教科書
説明粒度はここまで

CDCを構築・マネジメントするには

これであなたも明日からCDCを構築・マネジメントできますね！

CDCを構築・マネジメントするには

これであなたも明日からCDCを構築・マネジメントできますね！？

本当にできますか？・・・

CDCを構築・マネジメントするには

サービスの説明

E-3. 脆弱性診断

どこの製品・サービスを用いるか
イメージが湧きますか？

守るべきシステムやネットワーク、アプリケーションに脆弱性が無いかをツールを使って確認する。プラットフォーム診断、Web アプリケーション診断、Web API 診断、スマートフォンアプリケーション診断など、目的に合わせた診断の種類を選択する。ツールでの確認であるため、精度の問題はあるものの、低コストかつ短期間で実施できるため、より多くのシステムに対する定期的な診断も行う。

出典:セキュリティ対応組織の教科書第3.2版

再掲載

なぜX.1060に着目したか

お客様

セキュリティ対策や運用ってどこがゴールですか？
何かいいチェックリストはないですか？
網羅的で完璧なセキュリティ対策がしたいです

セキュリティSI屋
NTTデータ 小坂

国際機関などが出しているフレームワークを活用すると
網羅的に書いてありますよ。X.1060とかどうでしょう。

具体的なこと書いてなくて余計分からなくなりました。。
例えばX.1060ならNTTデータはどこまでサポート出来ますか？

NTTデータは多くの項目でサポート可能です。
確かに抽象的で難しい部分もありますね。
サービスマップを作った方がいいですか？

イイですね！欲しいです。期待しいてます。
ついでに他社の情報もあると便利です。

X.1060マップ活用WGを始動

X.1060マップ活用WG始動の理由

- X.1060フレームワークを活用してもらう機会を増やしたい
- 網羅的にセキュリティ対策を行うハードルを下げたい
- 日本企業が導入しやすいサービスを中心に探していきたい

X.1060マップ活用WG(成果物)の効果

ロユーザ企業目線

- 自社のCDCに必要な製品やサービスがすぐに見つかる
- セキュリティ製品やサービスを組み合わせて効率的にCDCを運用できる
- 日本企業が網羅的なセキュリティ対策を実施していくこと

ロセキュリティ企業（提供者）目線

- セキュリティビジネス活性化
  - ユーザ企業へ製品やサービスを売り込みやすい
  - X.1060の知名度を使って、海外へビジネス展開できる

X.1060マップ活用WG FY25活動予定

6月　　：キックオフ
7月-9月　：X.1060勉強会/X.1060マップ作製
10月-12月：X.1060マップ作製/本ワーキングの中間成果を対外発表（予定）
1月-3月　：年度内成果物のブラッシュアップ

※毎月１回程度の定例会合の実施

X.1060マップ活用WG メンバー募集

始動して日が浅いWGです、
ご興味がある方はWG参加をご検討ください。

〇募集概要

- 本WGの趣旨にご賛同頂き、積極的にご参加・発言頂ける方
- 各種成果物の作成にご協力いただける方
- 毎月の部会出席を５０%以上可能な方
- X.1060マップの知識がなくても問題ありません、
  講習会実施/サポートいたします
- セールス/マーケティング職の方の積極的なご参加を
  お待ちしております

X.1060を用いた網羅的なセキュリティ対策を実施していきましょう