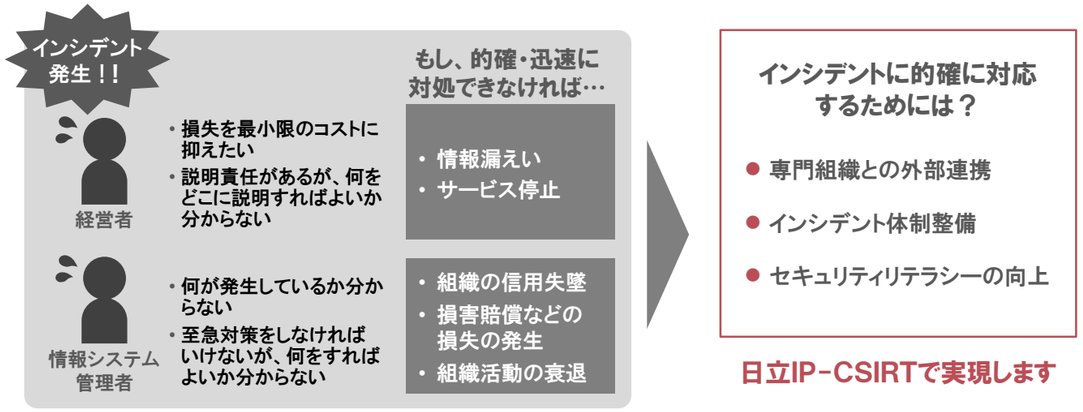
セキュリティインシデント対応サービス　Security incident response Service

インシデント対応サービス概要

インシデント発生時の対応は事前の対応体制の整備と的確な初動対応が重要なポイントとなります。
この実現に向けて、日立IP-CSIRT機能を組織化し、運用ルーチンワークとして対応することでセキュリティ対策を強化しております。

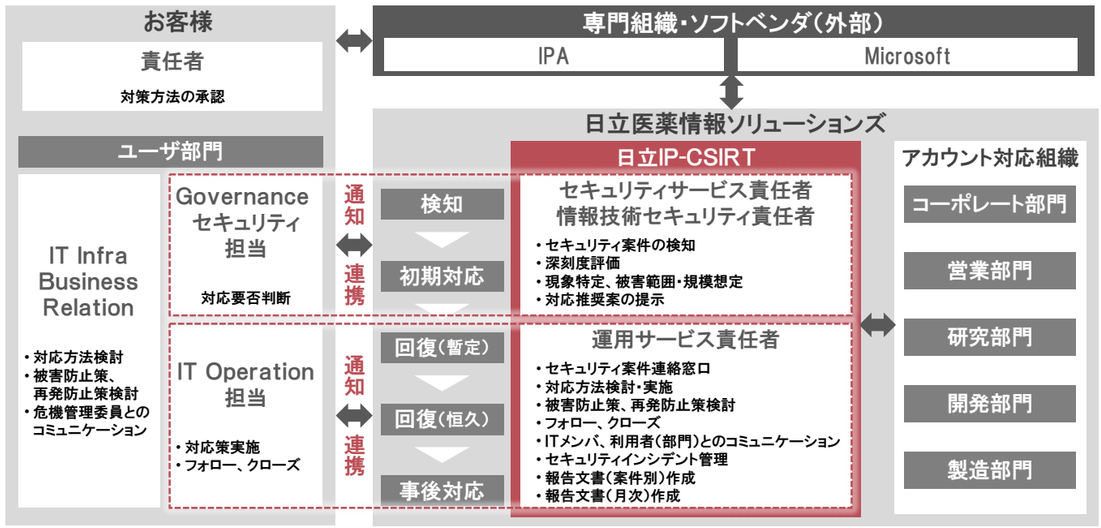


CSIRT（Computer Security Incident Response Team）とは？

- 「コンピュータセキュリティインシデント」に関する報告を受け取り、調査・対応活動を行う組織体の名称
- インシデントの影響の拡大を防ぎ、復旧措置や再発防止のための措置をとる一連の活動を実施

運用体制（一例）

一例として、下記のような役割分担にてセキュリティインシデントに対応致します。
日立IP-CSIRTにて、土日祝日を含む毎朝9：00に外部の専門組織の情報を確認し、緊急度の高いセキュリティ情報を入手した場合は6時間以内に日立推奨案を含む第一報を関係者に通知し、対応を進めます。



株式会社 日立医薬情報ソリューションズ
〒530-0005
大阪市北区中之島二丁目3番18号中之島フェスティバルタワー
TEL：06-4708-6630（代表）

お問い合わせ先

セキュリティソリューションサービス

HITACHI
Inspire the Next

「長年の経験」、「幅広いセキュリティ知識」、「有事の判断力」。セキュリティのエキスパートが、適正な運用管理を実現します。

お客様のビジネスを支える情報システム。その中でもセキュリティの運用管理は、システムリソースの増大、マルチベンダー化に伴い、複雑かつ多様化しています。また、情報漏洩リスクへの対策や、今後も拡大が想定されるサイバー攻撃に向けた対策を強化する必要性が高まってきています。

日立医薬情報ソリューションズでは、セキュリティの専門組織とも連携し、情報システム運用のプロフェッショナル要員による効率的な情報伝達と技術支援に努め、日常の運用業務からトラブル時の対処まで、お客様の円滑なセキュリティ運用管理をサポートします。

貴社のセキュリティ運用管理を見直しませんか？

- 経験豊富な情報システム運用のプロ集団により、セキュリティ運用をサポート
- マルチベンダーによる運用を整理統合して維持運用コストを削減
- 全体のセキュリティ対策を見直し、不足・過剰サービスを適正化

Solution & Service
日立医薬情報ソリューションズにお任せください。

サービスの特長　Merits of the Service

1. セキュリティ統制

1. 情報セキュリティマネジメント
2. アセスメント
3. インシデント対応サービス
4. 資産管理
5. 事業継続
6. 情報セキュリティ診断サービス

2. ネットワークセキュリティ

1. ファイアウォール
2. IDS/IPS
3. メール・Webフィルタリング
4. フィッシング対策
5. ウイルス対策
6. VPN

3. データセキュリティ

1. ID管理
2. 認証管理
3. アクセス制御
4. データ持出し制御，デバイス利用制御
5. 暗号化
6. ログ分析・保管

Point 1

全てお任せ！（All in one）

セキュリティに関してのコンサルティング・システム構築・運用管理まで全て一貫したサービスの提供が可能です。

Point 2

運用のプロによるサポート！

大手製薬業で経験を積んだセキュリティ運用のプロフェッショナルにより、被害の未然防止・関係者への迅速な情報伝達と技術支援に努めます。

Point 3

専門組織との連携！

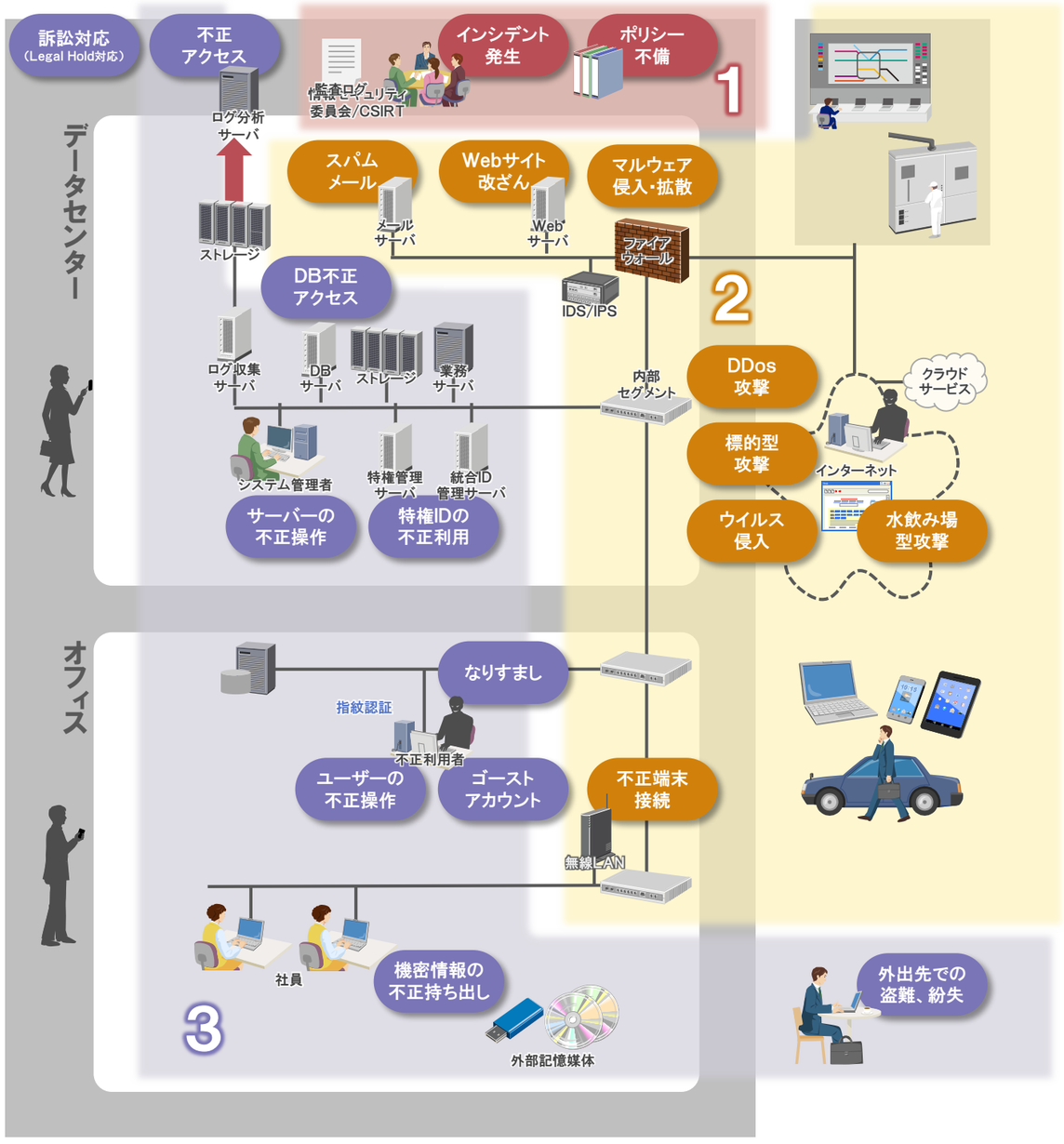
IPA*1、Microsoftといった外部専門組織や各ベンダと連携し、初動対応、事後対応、是正対応とします。
あらゆるステージでお客様をサポート

※1：US-CERTの正式名称は、United States Computer Emergency Readiness Teamです。／ ※2：IPAの正式名称は、Information-technology Promotion Agencyです。
※3：CSIRTの正式名称は、Computer Security Incident Response Teamです。

セキュリティリスクとサービス提供イメージ

Security risk & Image of the Service

オフィスやデータセンターには下図のような様々なセキュリティリスクが存在しています。
日立医薬情報ソリューションズでは ①セキュリティ統制、②ネットワークセキュリティ、③物理セキュリティ、④データセキュリティの以上4つのカテゴリーに分類したトータルソリューションをご提供し、あらゆるセキュリティリスクをカバー致します。



セキュリティ分類

1	セキュリティ統制
2	ネットワークセキュリティ
3	データセキュリティ

凡例：

：セキュリティリスク

サービス内容

Contents of the Service

サービス項目	対象となるリスク
1. セキュリティ統制	
情報セキュリティマネジメント(ISMS)	
・セキュリティポリシー策定	ポリシー不備
・Pマーク取得	
アセスメント	
インシデント対応サービス	
・セキュア情報検知サービス	
・セキュア情報提供サービス	
・インシデント管理サービス	
資産管理	
・構成管理	・インシデント発生 ・組織の信用失墜 ・損失発生(損害賠償) ・組織活動の衰退
・PCパッチ配信サービス	
・業務サーバパッチ適用サービス	
事業継続	
情報セキュリティ診断サービス	
・サーバ/OS診断	
・Webサイト診断	
・ソースコード診断	
・脆弱性診断サービス	
情報セキュリティ監査サービス	
2. ネットワークセキュリティ	
FW:ファイアウォール	
・FW	
・FWサービス	
PFW:パーソナルファイアウォール	
DBF:データベースファイアウォール	
WAF:アプリケーションファイアウォール	・DDos攻撃 ・ウイルス侵入 ・水のみ場型攻撃 ・標的型攻撃 ・不正端末接続
・WAF	
・WAFサービス	
VPN	
・IPSec-VPN	
・SSL-VPN	
・無線LANセキュリティ	
ネットワークIDS/IPS	
・IDS/IPS	
・IDS/IPSサービス	
メールフィルタリング	スパムメール
・メールフィルタリング	
・アンチスパム	
Webフィルタリング	マルウェア侵入・拡散
フィッシング対策	
ウイルス対策ソフト	
ウイルス対策ゲートウェイ	
ウイルス対策サービス	
改ざん検知・防止	Webサイト改ざん
・改ざん検知ソフトウェア	
・WORMストレージ	
・Web改ざん検知	

サービス項目	対象となるリスク
3. データセキュリティ	
ID管理	・DB不正アクセス ・特権IDの不正利用 ・ユーザーの不正操作 ・サーバーの不正操作 ・ゴーストアカウント ・なりすまし ・外出先での盗難・紛失
・統合ID管理	
・特権ID管理	
接続端末認証	
PKI認証基盤	
・認証基盤	
・認証ソフトウェア	
デバイス認証	
・ICカード・セキュリティデバイス	
・ワンタイムパスワード	
シングルサインオン	
・デスクトップシングルサインオン	
・Webシングルサインオン	
アクセス制御	
・ファイルサーバアクセス制御	
・OSリソースアクセス制御	
セキュアクライアント	
・シンクライアント化ツール	
・仮想化基盤	
・仮想化基盤監視	
アプリケーション起動制限	
DRM(デジタル利用権管理)	
データ持ち出し制御	
デバイス利用制御	
リダイレクト制御	
保存先制御	
ファイル・フォルダ暗号化	機密情報の不正持出し
HDD暗号化	
外部記憶媒体暗号化	
メール暗号化	
サーバ/DB暗号化	
暗号化ライブラリ	
ログ取得	・不正アクセス ・訴訟対応 (Legal Hold対応)
・クライアント	
・サーバ	
・ネットワークデバイス	
ログ分析・保管	
・Webレピュテーション	
・不正サイトリスト(Proxy、Mailログ)	
・アクセスログ	
統合ログ管理	