株式会社アイネット
DX本部
業務統括部
内海 章裕

会社概要

■商号　株式会社アイネット
■本社　横浜市西区みなとみらい3丁目3番1号
　　三菱重工横浜ビル23階
■設立　1971年4月22日（53期）
■資本金　32億円
■上場　東京証券取引所プライム市場 (証券コード:9600)
■社員数　連結:1,774名 単独:1021名 (2023年4月1日現在)
■売上　349億円 (2023年3月期連結)

第1データセンター（横浜）

第2データセンター（横浜）

第1データセンター

ISO 9001 JQA-QM6329　ISO 14001 JQA-EM6606　ISO/IEC 27001 JQA-IM0093

第2データセンター

ISO 9001 JQA-QM6329A　ISO 14001 JQA-EM6606A　ISO/IEC 27001 JQA-IM0093A

たいせつにします プライバシー 11820061(12)

子育てサポートしています 2012年認定事業主

woman act. 女性が、どんどん主役になる。 かながわ女性の活躍応援団

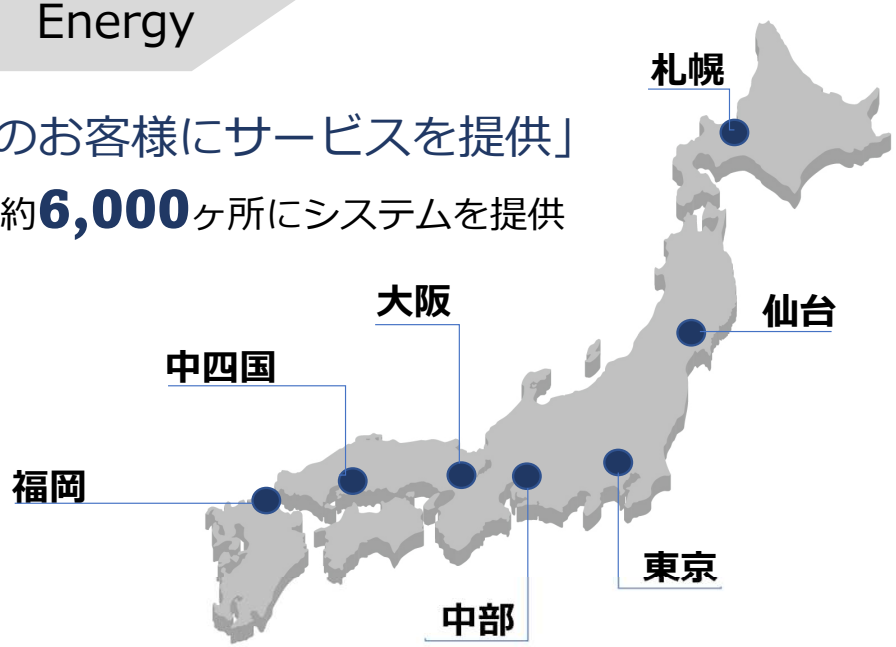
SS

エネルギー事業

Energy

「全国のお客様にサービスを提供」

SS全国約**6,000**ヶ所にシステムを提供



One Stop Service

DX

システムインテグレーション事業

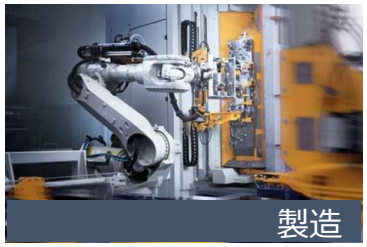
System Integration


金融


サービス


小売り・流通


宇宙


製造


建設・不動産


鉄道・交通インフラ


医療

DC

クラウドサービス事業

Cloud Services

Next Generation EASY Cloud®

クラウド基盤

仮想デスクトップサービス

VIDAAS®
Private Cloud Desktop as a Service

Cloudstor®
Private Cloud HDFS Storage Service

ファイル共有サービス

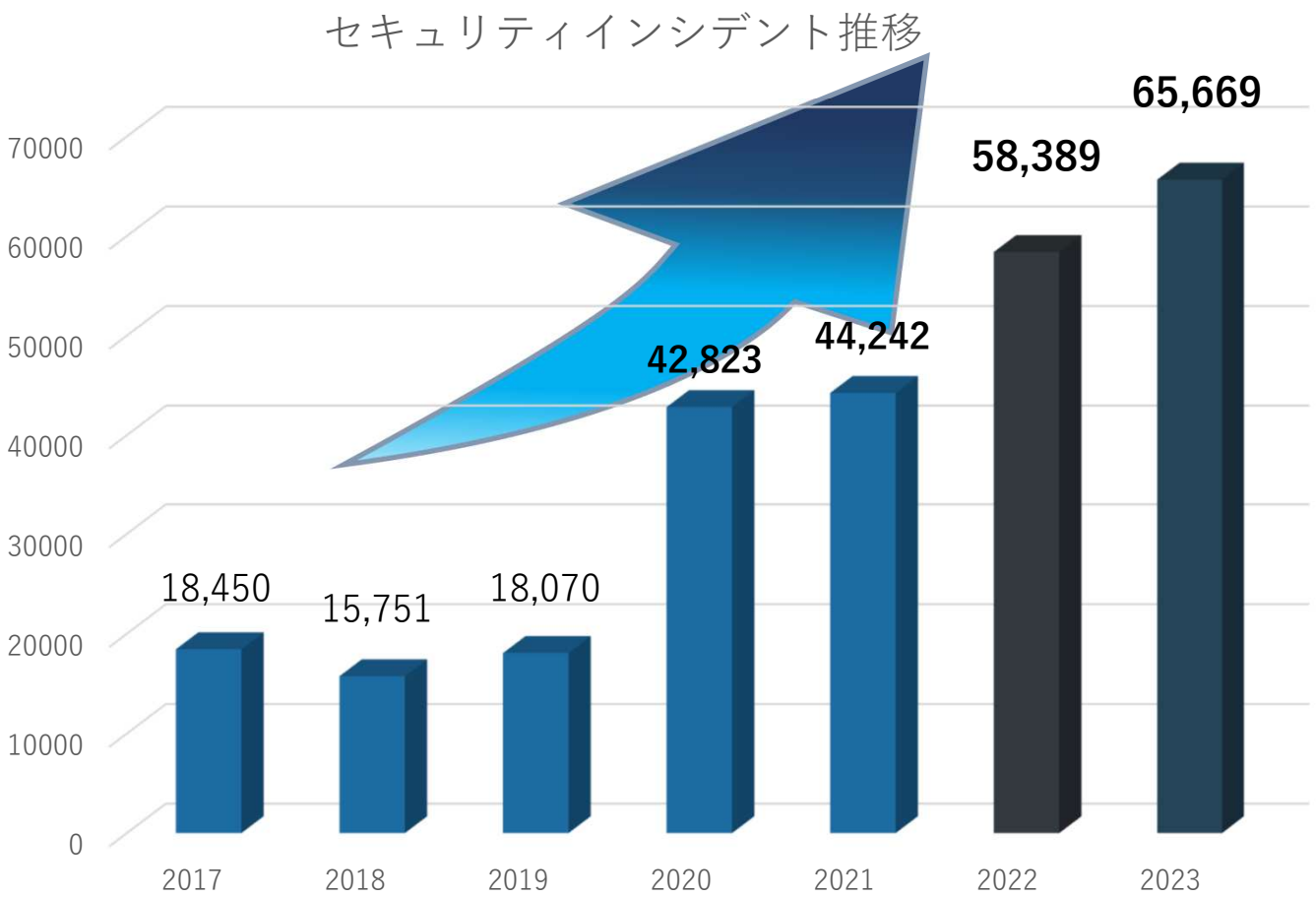
名刺管理サービス

名刺情報管理サービス
名刺バンク

Dream Drone®

ドローンプラットフォーム

セキュリティインシデント推移



※「JPCERT/CC インシデント報告対応レポート」を基にinetが編集

巧妙化・高度化する**サイバー攻撃**により
近年増加傾向の
セキュリティインシデント件数

セキュリティ動向

JPCERT/CC インシデント報告対応レポート（抜粋）

インシデントの種類	2022/10/1 ～12/31	2023/1/1 ～3/31	2023/4/1 ～6/30	2023/7/1 ～9/30	2023/10/1 ～12/31
ランサムウェアによる被害	39.9%	40.1%	43.5%	56.4%	56.3%
標的型攻撃（不正アクセス）	30.5%	28.1%	21.9%	17.8%	22.8%
クラウドサービスの不正利用	15.6%	16.9%	18.5%	13.5%	16.7%
内部不正による情報漏えい	0.1%	4.8%	13.3%	9.7%	2.1%
個人情報の窃取	0.1%	0.4%	0.4%	0.4%	0.3%
ビジネスメール詐欺	0.3%	0.4%	0.2%	0.6%	0.1%
DoS/DDoS	2.1%	0.3%	2.1%	1.6%	1.8%

70%～80%

20%以下

◆テレワーク普及の影響もあり、<u>セキュリティインシデントはここ数年再び増加傾向にある</u>

【社内】社内システムの脆弱性をスキャン　→　セキュリティホールのあるシステムを攻撃

【社外】テレワーク中のPCを狙った攻撃が増加　→　添付メールの開封によるランサムウェアへの感染増加

セキュリティ動向

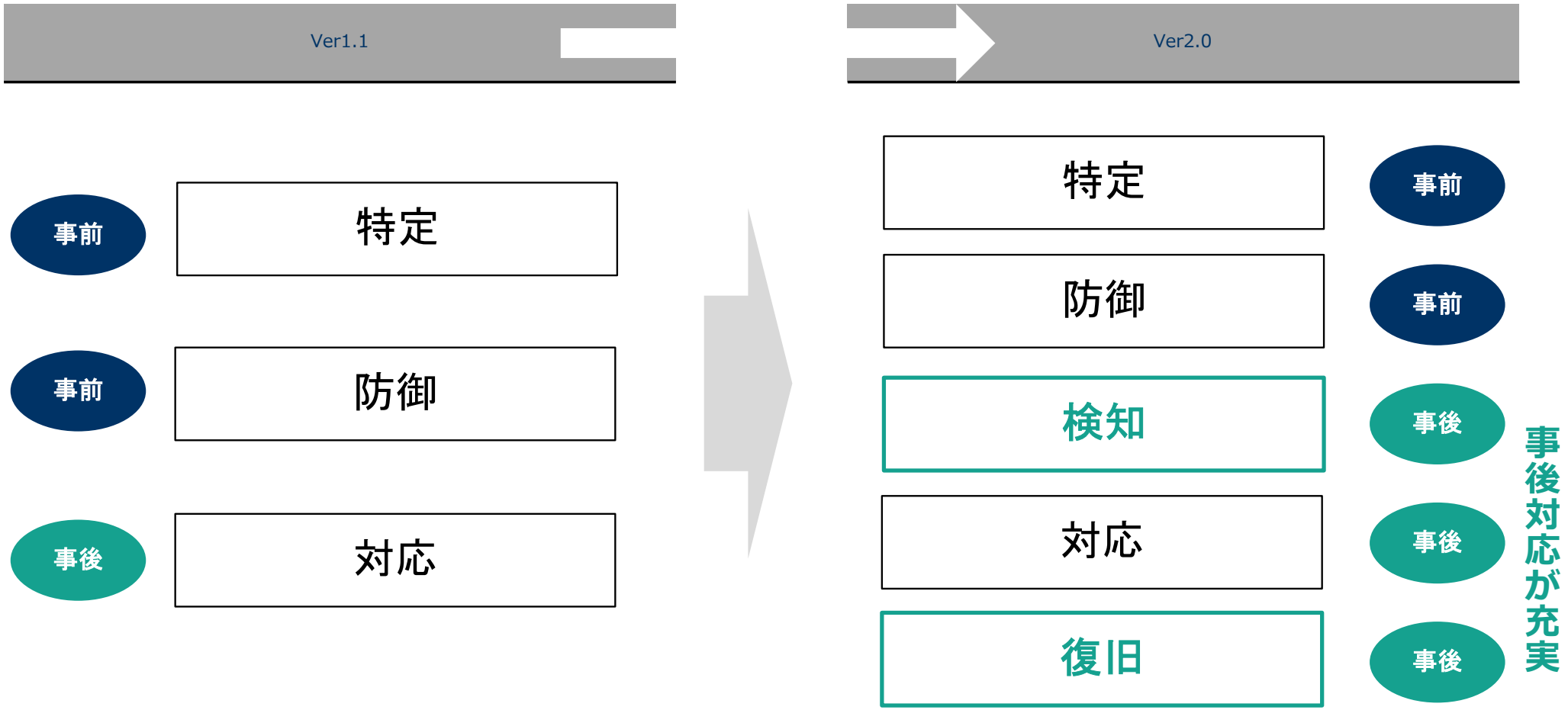
サイバーセキュリティ経営ガイドライン

Ver1.1		Ver2.0	
特定	(1) セキュリティポリシーの策定	特定	(1) セキュリティポリシーの策定
特定	(2) サイバーセキュリティリスク管理体制の構築	特定	(2) サイバーセキュリティリスク管理体制の構築
特定	(3) リスクの把握、対策目標と計画の策定	防御	(3) セキュリティ対策のための資源確保
防御	(4) PDCAの実施と対策の開示	防御	(4) リスクの把握、対策目標と計画の策定
特定	(5) サプライチェーンセキュリティ対策の実施	検知	(5) リスク対応策（防御・検知・分析）の実施
防御	(6) セキュリティ対策のための資源確保	対応	(6) PDCAの実施と対策の開示
特定	(7) ITシステム管理の委託範囲の特定	対応	(7) 緊急時の対応体制の整備
特定	(8) 情報共有活動への参加	復旧	(8) 復旧体制の準備
対応	(9) 緊急時の対応体制の整備	特定	(9) サプライチェーンセキュリティ対策の実施
対応	(10) 被害発覚後の準備	特定	(10) 情報共有活動への参加

出典：経済産業省「サイバーセキュリティ経営ガイドライン 改定のポイント」http://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

セキュリティ動向

サイバーセキュリティ経営ガイドライン



出典：経済産業省「サイバーセキュリティ経営ガイドライン 改定のポイント」http://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

セキュリティ動向

サイバーセキュリティ経営ガイドライン

Ver2.0		Ver3.0	
特定	(1) セキュリティポリシーの策定	特定	(1) セキュリティポリシーの策定
特定	(2) サイバーセキュリティリスク管理体制の構築	特定	(2) サイバーセキュリティリスク管理体制の構築
防御	(3)セキュリティ対策のための資源確保	防御	(3) セキュリティ対策のための資源確保
防御	(4)リスクの把握、対策目標と計画の策定	防御	(4) リスクの把握、対策目標と計画の策定
検知	(5)リスク対応策（防御・検知・分析）の実施	対応	(5) リスク対応策（効果的に対応する仕組み）の構築
対応	(6) PDCAの実施と対策の開示	対応	(6) PDCAの実施と対策の継続的改善
対応	(7) 緊急時の対応体制の整備	対応	(7) 緊急時の対応体制の整備
復旧	(8) 復旧体制の準備	復旧	(8) 事業継続、復旧体制の準備
特定	(9) サプライチェーンセキュリティ対策の実施	特定	(9) サプライチェーンセキュリティ対策の実施
特定	(10) 情報共有活動への参加	特定	(10) 情報の収集、共有及び開示の促進

出典：経済産業省「サイバーセキュリティ経営ガイドライン 改定のポイント」http://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

セキュリティ動向

サイバーセキュリティ経営ガイドライン

Ver2.0

Ver3.0

事前 特定

事前 防御

事後 検知

事後 対応

事後 復旧

NEW 構築

NEW 継続

NEW 共有

事業継続させる仕組み作りと
情報共有開示が追加

出典：経済産業省「サイバーセキュリティ経営ガイドライン 改定のポイント」http://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

セキュリティ動向

セキュリティ対策トレンドとキーワード

今求められるのは、事前防御型ではなく、事後対応型

Resilience
Resilient Security

回復力 / 回復力のあるセキュリティ

レジリエンス
被害の発生を前提とし
「検知・復旧の速度」に重点を置く考え方

ZERO TRUST
ZERO TRUST MODEL

信頼しないこと前提
信頼せずに必ず検証確認する

ゼロトラスト
侵入されることを前提にした考え方

ShadowIT

企業・組織側が把握せずに従業員または部門が
業務に利用しているデバイスや
クラウドサービス等のこと

シャドーIT
企業が認めていない
端末やサービスを社員が使ってしまうこと

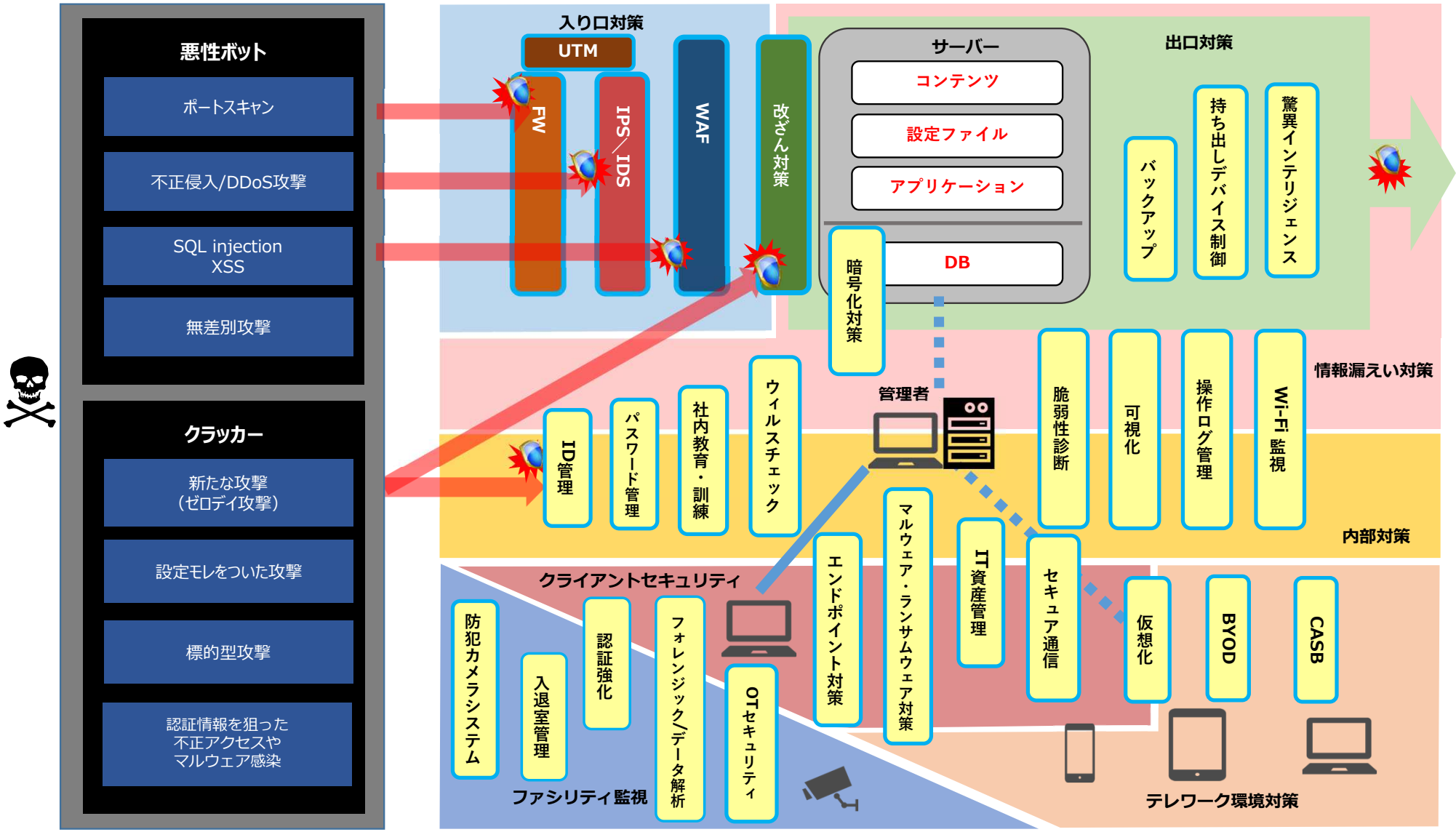
企業を取り巻くあらゆるリスク

企業が今、取り組むべきこと

対策

- DR：災害復旧
  (Disaster Recovery)
- BCP：事業継続計画
  (Business Continuity Plan)

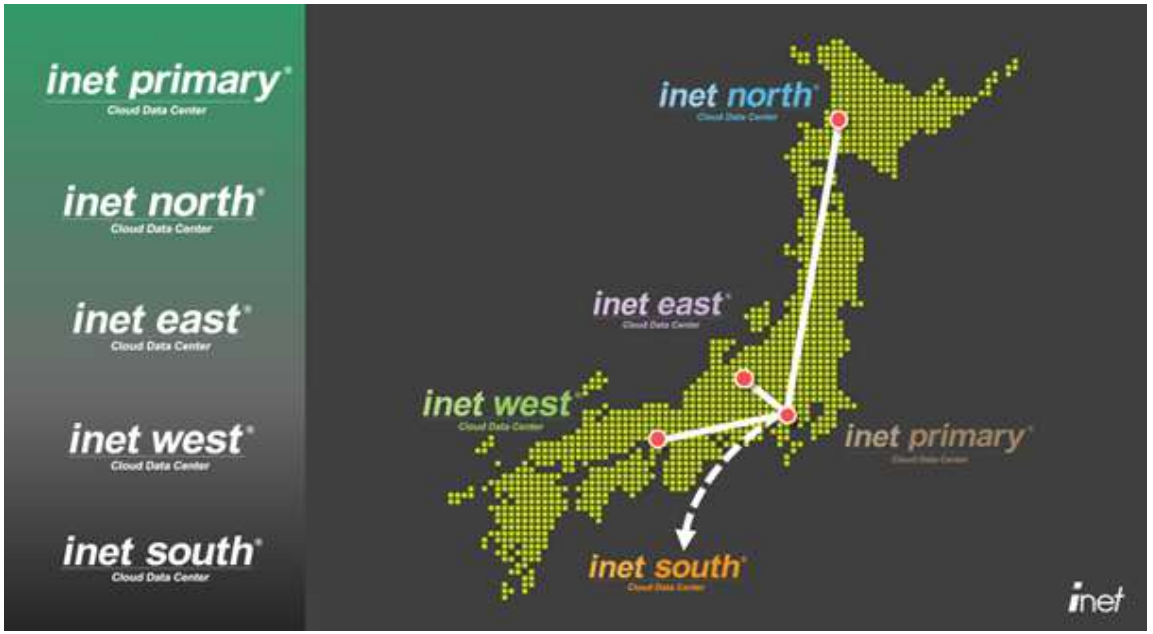
セキュリティ全体図


悪性ボット
ポートスキャン
不正侵入/DDoS攻撃
SQL injection
XSS
無差別攻撃
クラッカー
新たな攻撃
（ゼロデイ攻撃）
設定モレをついた攻撃
標的型攻撃
認証情報を狙った
不正アクセスや
マルウェア感染
入り口対策
UTM
FW
IPS／IDS
WAF
改ざん対策
サーバー
コンテンツ
設定ファイル
アプリケーション
DB
暗号化対策
出口対策
バックアップ
持ち出しデバイス制御
驚異インテリジェンス
情報漏えい対策
管理者
ID管理
パスワード管理
社内教育・訓練
ウィルスチェック
脆弱性診断
可視化
操作ログ管理
Wi-Fi 監視
内部対策
クライアントセキュリティ
防犯カメラシステム
入退室管理
認証強化
フォレンジック/データ解析
OTセキュリティ
エンドポイント対策
マルウェア・ランサムウェア対策
IT資産管理
セキュア通信
仮想化
BYOD
CASB
ファシリティ監視
テレワーク環境対策

自社“**データセンター**”からセキュリティサービスをご提供

首都圏　　：**inet primary**
北海道地区：**inet north**
長野地区　：**inet east**
関西地区　：**inet west**

**4拠点のデータセンター
すべてに当社の
マネージドクラウド基盤を設置**



今後もアイネットは、セキュリティサービスの拡充と
お客様ニーズにお応えするサービスのご提供を行って参ります。

＜問い合わせ先＞
株式会社アイネット
DX本部 業務統括部 セールスサポート室

E-Mail：security-sol@inet.co.jp
TEL：03-5480-3500