情報セキュリティ総合戦略について

株式会社リテックでは、業務において取り扱う、ステークホルダーに関する情報
（特に個人情報・プライバシー・企業秘密）の重要性から、様々な
情報セキュリティに関する対策に取組んできました。
近代のインターネットの市民レベルでの普及・コンピューターウイルスの高度化や
企業内部からの情報漏洩等の、IT 社会における事故は日々多発・多様化しております。
また、人的犯罪におけるハード面（施設・機器類）の防犯対策もより重要であります。
以下・これまでの私共の取組みと今後の戦略を明示します。

施設面における、人的防犯対策について	● 事務所の机・書棚は全て施錠。
IT 機器における、防犯対策について	● 全パソコンに、最新ウイルス対策ソフトを導入。 ● 全パソコンに暗証番号によるアクセス制御を導入。 ● パソコンは持出禁止。
情報媒体の管理について （但し、電子・紙媒体を含む。）	● 情報媒体（MO,FD）は施錠管理すると共に、持出禁止。 ● 従業員名簿、取引先名簿は、総務部が保管するが、顧客訪問時以外は持出禁止。 ● 破損した媒体はシュレッダーにて物理的に破壊する。
情報管理に関する、具体的取り組み。	● 各担当が保有する情報は、業務受注と終了後､その都度個別受注契約書類及び業務全体の進行記録ファイルに記載することによって総務部で､一元管理をしている。
破棄すべき、情報の見極めについて。	● アフターサービスについて、過去 10 年以前のものは破棄。 ● 個人情報は、6 月以前のものは破棄。 ※但し、証拠保全の必要があるものは除く。
情報管理におけるＣＳＲの教育訓練について	●H29/11/28 ＣＳＲ研修実施。（総務部） ＣＳＲ活動実績の確認（総務部主導。会社全体）

緊急時の対応（情報媒体に関する漏洩、ウィルス感染等の事故への対応）	● 媒体の対象である本人に告知。２次被害を防止すると共に、管轄官庁へ報告し、指示を求める。 ● 当方に法的責任がある場合は損害保険の適用を検討する。
緊急時の対応（施設への人的侵入、機器の破損等） （天災、流行病等避けざるを得ない事由）	● 警察、消防への通報。 ● 大地震等の天災の場合は安全が確認できるまで業務休止。管轄官庁の指示を求める。 ● 流行病（新型インフルエンザ）の感染がパンデミックに達した場合は、事態が収拾する迄、業務休止する。また感染予防策として N95,9211 レベルのマスクを全員に配布する。 ● 感染の恐れがある者については、自宅で待機させる。 ● 顧客情報の漏洩等において、当方に法的責任がある場合は損害保険の適用を検討する。
潜在的不祥事への対応	●雇用契約書及び誓約書において職員に顧客、従業員の個人情報ならびに企業秘密の守秘義務を課している。 ●違反への損害賠償請求を担保している。

ＣＳＲ実施責任者　大野公靖

平成 26 年 10 月 1 日改訂